International Telecommunication Union

ITU-T

Technical Specification

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(June 2020)

FG-NET2030 – Focus Group on Technologies for Network 2030

Network 2030 Architecture Framework

FG NET-2030 Technical Specification on

Network 2030 Architecture Framework

Table of Contents

List of Figures

List of Tables

FG NET-2030 Technical Specification on

Network 2030 Architecture Framework

Acknowledgement

The contributions from the following individuals are much appreciated by the FG NET2030:

Mehmet Toy, Alex Galis, Adrian Perrig, Yingzhen Qu, Jingcheng Zhang, Ning Wang, Yan Shen, Dharmendra Misra, Toerless Eckert, Stewart Bryant, David Hutchison, Uma Chunduri, Daniel King, Dirk Trossen, Liang Geng , John Day, Alexander Clemm, Mehdi Bezahaf, Yuexia Fu, Cheng Zhou, Hongwei Yang, Huijuan Yao, Padma Pillay Esnault , Christian Esteve Rothenberg, Jyrki Penttinen.

1. Summary

This technical specification begins describing architectural principles and overall architecture for public networks in the year 2030 and beyond, namely Network2030. Later, the specification elaborates on the details of access/edge architecture, routing and addressing, data path security, quality of service (QoS), burst switching, network slicing, Multi-access Edge Computing (MEC) federation, and network management for Network2030. Impact of quantum computing is also addressed.

2. Keywords

Network 2030, architecture, principle, access, edge, data path, network slicing, application, connectivity, OSS/BSS, NFVO, VNFM, VIM, UNI, ENNI, MEC, routing, security, burst switching, QoS, scalability, in-time service, on-time service, federation

3. Scope

FG-NET2030 is formed to address expected uses cases, services, technologies; and identify requirements and architecture for public networks in the year 2030 and beyond, namely Network2030. This specification is focused on the Network2030 architecture and its details as summarized in Section 2. The Network2030 use cases, services, technologies and requirements are addressed in [Sub-Group 1.1, Sub-Group 2.1, Sub-Group 2.2].

4. Abbreviations

AAA – Authentication, Authorization and Accounting

AI- Artificial Intelligence

B5G- Beyond 5G

BIER- Bit Index Explicit Replication

BSS-Business Support Systems

DN – Data Network

E/AO- Edge/Access Operator

eCPRI- Enhanced Common Public Radio Interface

ENNI- External Network Network Interface

FEC- Forward Error Correction

FRR- Fast Re-Route

iBGP- Interior Border Gateway Protocol

IGP- Interior Gateway Protocol

IoT- Internet of Things

ISR- Interrupt Service Routine

KPI- Key Performance Indicator

LSO- Lifecycle Services Orchestration

LSVR- Link State Vector Routing

MEC – Multi-access Edge Computing

ML- Machine Learning

MSDC- Massively Scaled Data Center

MSS- Maximum Segment Size

NFVO- Network Functions Virtualization

NS- Network Slicing

PDU- Protocol Data Unit

OSS- Operations Support Systems

QFC- Quantum Flow Control

QoS- Quality of Service

QUIC- Quick UDP Internet Connections

RCS - Rich Communication Services

RPKI- Resource public-key Infrastructure

RTT- Round Trip Time

SCION- Scalability, Control, and Isolation on Next-Generation Networks

SFC- Service Function Chaining

SP- Service Provider

TCP- Transmission Control Protocol

TSN- Time-sensitive Networking

UE- User Equipment

UTRAN- UMTS Terrestrial Radio Access Network

UNI- User Network Interface

VIM- Virtual Infrastructure Manager

VM- Virtual Machine

VNF- Virtual Network Function

5. Conventions.

None

6. Definitions and Acronyms

Term	Definition	Reference
Accessibility	It represents the degree to which a system, device, service, or environment is available to as many people as possible. Accessibility can be viewed as the "ability to access" and benefit from some system or entity.	This document
Access Network	Access network is last mile connectivity to the consumer device. Access network may be Mobile Radio, copper, fibre, satellite or terrestrial floating network	
Application Interface	Application UNI or Application ENNI	This document
Applications and Business Service Viewpoint	It focuses on the explain and justifying the role of applications and services with the user/tenant organization as well with the impact on the infrastructure.	ISO/IEC JTC1/SC21/WG7
Architecture	It is a plan for implementing non-functional and functional requirements within the system limits/boundaries. It is conceptual model that defines the structure, behavior, and a number of views (i.e. Physical Resources view, Logical & Functional View, Control view, Management View, Information View, Applications & Business View) of a system within the system limits.	ISO/IEC JTC1/SC21/WG7
Architecture Principle	A principle is a rule that governs how something is to be done; in the case of network infrastructure architecture, principles are used as a basis for the design and operation of the system. Each principle will apply to a particular set of viewpoints on the architecture. It is an instruction that has to be followed or is an inevitable consequence the way that a system is constructed. From the user point of view the principles of a system are understood as the essential characteristics of the system, and/or reflecting system's purpose, and/or the effective operation, and /or use of which would be impossible if any one of the principles was to be ignored. Examples of use of principles are a) a system may be explicitly based on and implemented from principles; b) systems can be measured /compared / evaluated based on a set of principles; c) systems values that are underling behavior & operations.	This document
Architectural viewpoints	They are a reflection of the viewpoints, initially identified in RM-ODP specification (ISO/IEC JTC1/SC21/WG7, titled “Reference Model of Open Distributed Processing” shorthand RM-ODP, dated 1997 SO-IEC JTC1/SC21/WG7 (www-cs.open.ac.uk/~m_newton/odissey/RMODP.html)	ISO/IEC JTC1/SC21/WG7
Availability	It represents the degree to which a system is in a specified operable and committable state at the start of a task. It is the proportion of time a system is ready for use.	This document
Burst Forwarding	The burst forwarding is an application-aware data forwarding technology. A burst is the basic data unit that	This document

Term	Definition	Reference
	can be processed by the application. The content of the burst is application dependent. For example, a burst can be a photo in the image processing system, or it can be a video clip in the video streaming service. The burst forwarding network uses burst as the basic transmission unit. The data source sends the entire burst using the line rate of the network interface card.	
Certification	It refers to the confirmation of certain characteristics of an object, element of system. This confirmation is often, but not always, provided by some form of external review, assessment, or audit.	This document
Cloud Operator	An entity that is responsible for making applications available to users. It can be public or private. •	This document
Connectivity Operator	An intermediary that provides connectivity between Cloud Operators, Connectivity Operators, and users. In case of Internet, the Connectivity Operator is a public network provider.	This document
Consumer Device	Consumer Device is a generic term used in this document that implies any device that consumes service offered by communication network either in autonomous fashion or as a human operated/controlled function. Examples include 3GPP Mobile Terminals (MT), IoT/MTC device, Autonomous Sensors/Controllers, Space communication terminals, Broadband Forum Network Terminators (NT) or Home gateway, Customer Edge router, Cable STB, CPE, Satellite phones or any such future emerging device	This document
Consumer Device Interworking	Consumer device inter-working refers to peer to peer communication as direct communication channel or through access/edge network segment of communication network	In this document
Controller (SDN architecture-based)	The satellite network system may also employ hierarchical architecture. So, some of the satellite not only play the role of router but also controller. Refer to SDN, the MEO and GEO may stand higher layer and control the low layer devices (LEO) which are expected to take the role of data forwarding in the data plane.	This document
Control plane	The set of functions that controls the operation of entities in the stratum or layer under consideration, plus the functions required to support this control.	ITU-T Y.2011
Data Network	Data Network that is used in generic form to connect two networks or a network with some application function	This document
Data plane	The set of functions used to transfer data in the stratum or layer under consideration.	ITU-T Y.2011

Term	Definition	Reference
Data privacy	Restricting the distribution of data to only authorized parties.	In this document
Domain	An administrative domain is a collection of systems and networks operated by a single organization or administrative authority. Infrastructure domain is an administrative domain that provides virtualized infrastructure resources such as compute, network, and storage or a composition of those resources via a service abstraction to another administrative domain and is responsible for the management and orchestration of these resources.	ETSI NFV MANO
Edge/Access Operator	An operator that provides edge computing and/or access networking.	This document
Edge Network	Edge network is typically considered segment of the network after access network and before aggregation point in core network. But it is not strictly fixed. A SP or E/AO can shift the edge contour to very close to customer device e.g. collocated with gNodeB or can have at some distance. Sometime it depends upon the type of network operator or industry vertical solution provider as well. Another view is the point of demarcation between one operator or SP to another operator or SP or enterprise.	
Edge Interworking	Edge interworking refers to Edge to Edge communication between communication service provider networks or between Industry vertical solution and communication service provider networks	This document
Functional Entity	An entity that comprises an indivisible set of specific capabilities. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.	ITU-T Y.2012
Functional Requirement	It is a description of what a system/infrastructure is supposed to do and it defines a function, or a feature of a system, or its components, capable of solving a certain problem or replying to a certain need/request. The set of functional requirements present a complete description of how a specific system will function, capturing every aspect of how it should work before it is built, including information handling, computation handling, storage handling and connectivity handling. The use of Functional and Non-functional Requirements include a) explanation on what has to be done by identifying the necessary integration of systems structure and systems behavior; b) Verification as implementation of the requirements can be determined through basic possible methods: inspection, demonstration, test or analysis.	This document
Ground Station and Terminal	Ground station and terminals are a type of physical terrestrial devices that act as gateway or interfaces between terrestrial and space networks through radio communications. At present, the networking mechanisms and protocols used in space networks are different from that in the traditional IP framework in the	This document

Term	Definition	Reference
	terrestrial infrastructures, and hence ground stations and terminals have been responsible for protocol translations and creation/maintenance of tunnels in order for data packets to traverse different network environments.	
High-Precision Network Services	Network services that support stringent service level objectives at very high precision that is explicitly specified, such as in-time and on-time latency guarantees.	ITU-T FG NET-2030 SubG2 Deliverable
IMT-2020 or Network 2030 Planes	A plane is a subdivision of the specification of a complete IMT-2020 or Network 2030 systems, established to bring together those particular pieces of information relevant to some particular area of concern during the analysis or design of the system. Although separately specified, the planes are not completely independent; key items in each are identified as related to items in the other planes. Each plane substantially uses foundational concepts. However, the planes are sufficiently independent to simplify reasoning about the complete system specification. Examples are data plane, control plane, management plane, service plane, intent plane, information and knowledge plane, user plane.	ITU-T IMT 2020
Infrastructure information Viewpoint	It focuses on models and frameworks to present the information requirements and control information of a system. It would show how information is partitioned across logical boundaries and the required quality attributes of information.	ISO/IEC JTC1/SC21/WG7
Integrability	It represents the process of bringing together the component sub-systems into one system (an aggregation of subsystems cooperating so that the system is able to deliver the overarching functionality) and ensuring that the subsystems function together as a system. Integrability is based on a dynamic interaction between groups subsystems and in all parts of the system.	
In-Time Service	In-time Services are services where packets need to be delivered within maximum latency allowed for packet delivery. Packets may be delivered at any time before or until the maximum latency. Multimedia applications supporting buffering capabilities are typical applications that use in-time services.	IMT2030 Sub Group 2 doucment
Key Performance Indicators (KPIs)	Performance indicator is describing the degree of performance of a system according to certain predefined metrics. It defines a set of values against which to measure network functions and/or network operations.	ITU-T Y.4900/L.1600
Logical & Functional Viewpoint	It focuses on the models, mechanisms and frameworks for describing the operations and functions/ virtual functions of a system in an implementation independent way. It includes the operations on information and on the control of information for e2e operations, including information transfer, retrieval,	ISO/IEC JTC1/SC21/WG7

Term	Definition	Reference
	transformation, adaptation and methods necessary to automate the infrastructure processing.	
Logical Resource	An independently manageable partition of a physical resource, which inherits the same characteristics as the physical resource and whose capability is bound to the capability of the physical resource. NOTE – "independently" means mutual exclusiveness among multiple partitions at the same level.	ITU-T Y.3011
Maintainability	It is a characteristic of design and installation, expressed as the probability that an element of a system will be retained in or restored to a specified condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources.	This document
Management Functions	The functions or operations related to the management of the network functions and resources. NOTE -Overall coordination and adaptation for configuration and event reporting are achieved between network function infrastructure and network management systems. It includes the collection and forwarding of performance measurements and events. Network function lifecycle management is included with network function instance management. The network management system is authorized to exercise control over and /or collect management information from another system. It is tightly connected with BSS/OSS such that the most efficient and effective way to access, control, deploy, schedule and bind resources is chosen as requested by customers.	ITU-T IMT-0-040
Management Plane	The set of functions used to manage entities in the stratum or layer under consideration, plus the functions required to support this management.	ITU-T Y.2011
Midhaul	It is network segment between fronthaul and backhaul.	GSM
Mobile Edge Computing (MEC) server	MEC has been a terminology mainly in the context of 5G where local computing and storage capabilities can be embedded at the mobile network edge in order to provide low latency data/computing services to locally attached end users. It can be envisaged that in future emerging space and terrestrial networks, LEO satellites can also become MEC servers in constellation in the space once equipped with computing and data storage capabilities.	This document
Network2030	System, system components and associated aspects that relate to an integrated, highly automated, intelligent partitions of the infrastructures (including heterogeneous communication, compute, storage and network services/applications resources), which contain a number of operator operational domains in all network segments (wired/wireless access, core, edge, space or mixture of segments), that may be accessed by a user from one or more locations.	This document
Network function	A processing function in a network. It includes but is not limited to network nodes functionality, e.g. session management, mobility management, switching, routing	ITU-T IMT-0-043

Term	Definition	Reference
	functions, which has defined functional behavior and interfaces. Network functions can be implemented as a network node on a dedicated hardware or as a virtualized software function.	
Network slice	A complete end-to-end logically partitioned network providing dedicated telecommunication services and network capabilities. The behavior of the network slice is realized via network slice instance(s).	ITU-T IMT-0-043
Network Orchestration	An automated arrangement, governing, coordination of complex network systems and functions including middleware for both physical and virtual infrastructures. It is often discussed as having an inherent intelligence or even implicitly autonomic control. Orchestration results in automation with control network systems.	ITU-T IMT-0-040
Network Slicing (NS)	It is an end-to-end concept covering all network and cloud network segments (access, core, transport, edge). It enables the concurrent deployment of multiple logical, self-contained and independent shared or partitioned network resources and a group of network and service functions on a common infrastructure platform. **Network Slicing** is a management mechanism that a resource provider can use to allocate dedicated partition infrastructure resources and service functions to users.	This document
Network Slice	It can be defined as a set of infrastructures (network, cloud, data center) components/network functions, infrastructure resources (i.e., connectivity, compute, and storage manageable resources) and service functions that have attributes specifically designed to meet the needs of an industry vertical or a service. As such a **Network Slice** is a managed group of subsets of resources, network functions/network virtual functions at the data, control, management/orchestration, and service planes at any given time. The behavior of the **Network Slice** is realized via network slice instances (i.e., activated slices, dynamically and non-disruptively re-provisioned). **Network Slices** considerably transform the networking perspective by abstracting, isolating, orchestrating, softwarizing, and separating logical network components from the underlying physical network resources and as such they are inter-twined to enhance Internet architecture principles.	This document
Network Softwarization	Network softwarization is an overall transformation trend for designing, implementing, deploying, managing and maintaining network equipment and network components by software programming, exploiting characteristics of software such as flexibility and rapidity of design, development and deployment throughout the lifecycle of network equipment and components, for creating conditions that enable the re-design of network and services architectures; allow optimization of costs and processes; and enable self-management.	ITU-T O-016
Non-functional Requirement	It is a specification criterion that can be used to judge the operation of a system/infrastructure, rather than specific behaviors; it is a description of how well a system performs its	This document

Term	Definition	Reference
	functions; it represents an attribute that a specific system must have. The non-functional requirements are controlled by other aspects of the system. Examples of non-functional requirements are accessibility, availability, certification, consistency, compliance, determinism, extensibility, fault tolerance, integrability, interoperability, maintainability, operability, performance, privacy, resilience, reliability, robustness, scalability, security.	
Network Virtualization	A technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collection of multiple virtual networks can simultaneously coexist over the shared networks. This includes the aggregation of multiple resources in a provider and appearing as a single resource.	ITU-T Y.3011
On-Time Services	On-time Services are services that ensure the arrival of packets within a specific time window. On-time services need packet delivery within maximum and minimum limit of latency. A packet must be delivered no later than upper bound of the time window, but also no earlier than the lower bound of the time window	IMT2030 Sub Group 2 document
Operability	It is the ability to keep a system in a safe and reliable functioning condition, according to pre-defined operational requirements. It is the ability of system components to work together to accomplish a common task such as startup, running, decommission of components part of network life-cycles network stages.	This document
Path-aware networking (PAN)	The sender of a packet obtains information on the network path the packet will follow to reach the destination. The network path information can be at different granularities, for instance at the AS level. The information can be obtained at the moment the packet is sent, for instance by embedding the network path in the packet header.	This document
Performance	It describes the degree of execution of a system (according to certain predefined metrics, e.g. convergence time).	This document
Physical Resource Viewpoint	It focuses on the models, devices, technical artefacts (realized components) and frameworks from which a system is build and as such it is describing the way to support all viewpoints, including the definition of physical distributions to realize different partitions identifies in the logical and functional viewpoint.	ISO/IEC JTC1/SC21/WG7
Privacy	It is the ability of system or actor to seclude itself or information about itself and thereby reveal itself selectively.	This document
QoS	Quality of Service is used to describe various functions in different contexts. QoS is used for the functionality that is most often referred to as QoS in the context of transport, networking or data-link layers: switch/router forwarding-plane functions that impact the absolute or differential drop behaviour, throughput and latency of individual packets and packet flows	This document

Term	Definition	Reference
	under uncongested or congested traffic load as well as the required control and management plane functions to support these forwarding-plane functions.	
Radio Access Network	Future network is expected to use heterogeneous wireless link layer to support multiple technologies & use cases. These aspects are considered under this section	This document
Reliability	It is the proportion of time a system will continue to function properly while it is being used. Specifications for reliability typically refer to stability, availability, accuracy, and maximum acceptable/tolerable bugs.	This document
Robustness	It is the ability of a system to cope with errors during execution or the ability of a system to continue to operate despite abnormalities in input or in environment context.	This document
RCS	Rich Communication Services. A term used by GSMA to define and group advanced communication services including voice/video call, chat & messaging, picture sharing, etc.	GSMA
Resilience	It is the ability to provide and maintain an acceptable level of system operations in the face of faults and challenges to normal operations.	This document
Satellite Low Earth Orbit (LEO)	Satellite has lower physical orbit which potentially bring the short latency benefit. Medium Earth Orbit (MEO) and Geostationary Orbit (GEO) can provide more physical stability. The current satellite system mostly provides relay function however in the future the satellite system may build up a mesh-like network then provide routing and forwarding function. The LEO should be organized as routing system and work as router. The MEO and GEO may also play the role of router but work as complement and control function further.	This document
Scalability	It is the capability of a system, or a process to handle a growing amount of work, or its potential to be enlarged to accommodate that growth.	In this document
Security	It is freedom from, or resilience against, potential harm (or other unwanted coercive change) caused by other systems. It uses protection mechanisms (e.g. mechanisms for controlling access of programs, processes, or users to resources) to prevent misuse of resources. Misuse defined with respect to policy a) preventing exposure of certain sensitive information, b) preventing unauthorized modification/deletion of data and c) need to consider external operational environment.	In this document
Service Provider	An entity that is responsible for the creation, delivery and billing of services, and negotiates relationships among Cloud Operators, Connectivity Operators, Space Operators, and Users. It is the single point of contact for the user.	This document

Term	Definition	Reference
Software-defined networking	A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.	ITU-T Y.3030
Space Operator:	An Operator that may provide connectivity as well applications in the space.	This document
System Design	It is a plan for implementing functional requirements.	This document
System Management Viewpoint	It focuses on the models, artefacts and frameworks describing the ways to manage, control and life cycle changes methods of all elements in the other viewpoints at the required management attributes and key performance indicators (KPIs). Note - The description of Network 2030 could be structured as a set of projections of the architecture onto models and specific artefacts representing these 5 viewpoints.	ISO/IEC JTC1/SC21/WG7
System boundaries / limits	They define the constraints and freedoms in controlling the system. Limits can be determined by analyzing how the behavior of the system depends on the parameters that drive the system. Some limits would lead to unexpected and significant behavior changes of the system, for example the unpredictable boundaries or changes in the scale of magnitude. Some other limits are determined by non-common behavior interactions between the components of a system.	ISO/IEC JTC1/SC21/WG7
User	A person or organization or a machine that maintains a business relationship with and uses service from a Service Provider, or just uses the public network for connectivity between his/her/its application.	[ARCH.1]
User plane	A synonym for the data plane. NOTE – "User plane" is also referred to as the "transport plane" in other ITU-T Recommendations.	ITU-T Y.2011
Virtualized Network Function	A network function whose functional software is decoupled from hardware and runs on a virtual machine(s).	ITU-T Y.3321
Virtual resource	An abstraction of physical or logical resource, which may have different characteristics from the physical or logical resource and whose capability may be not bound to the capability of the physical or logical resource.	ITU-T Y.3011

Table 1.

7. Introduction

The current Internet derives mainly from the 1980s and soon after. Among the key objectives were best effort connectivity and simplicity along with the ability to survive some level of link and node failures. Private networks have been used for applications requiring more assured security and privacy, and/or service quality better than best effort.

With the advent of new wireline and wireless technologies that are pushing the transmission rates from Mbps and Gbps to Tbps, the future network consisting of many types of integrated networks is expected to support applications requiring large bandwidth. Future Internet should no longer be a vehicle only for best effort connectivity, but a programmable infrastructure of connectivity and applications supporting vital and high precision services that require low latency, appropriate security, and extremely high reliability for communications between most of the locations in the world.

The number of connected devices is expected to grow to 28.5 billion in 2020 [GEN.1] and 100 billons in 2025[GEN.2], increasing the traffic from 33 zettabytes (i.e. 33 x 10^{21}) in 2018 to 175 zettabytes (i.e. 175 x 10^{21}) by 2025 [GEN3].

The intelligence is no longer only in the end devices, but distributed among end devices, data-centers, cloud, space, edge and core devices in the network. As a result, the complexity is increased. On the other hand, the automation of operational processes for inter and intra networks is being worked in the industry. Management of network elements and applications on-demand is becoming a common trend. The level of intelligence in each component is increased with the proliferation of machine learning (ML) and artificial intelligence (AI) techniques, and advances in memory and computing technologies. By 2030, we expect to see self-managed networks with substantial user controls and tremendous growth in the services supported by autonomous edge devices.

A new Internet architecture framework is necessary to support the conditions outlined above, and also to support the requirements for future applications and services.

This specification begins with describing architectural principles and overall architecture for Network2030, and then describes access/edge architecture, routing and addressing, data path security, quality of service (QoS), burst switching, network slicing, and network management for Network2030. Impact of quantum computing is also addressed.

8. Architecture Principles

Network 2030 refers to an integrated, highly automated, intelligent infrastructures which contain a number of operator operational domains in various types of network segments (e.g., wired/wireless access, core, edge and space segments). This integration is based on a dynamic interaction between groups of compute, storage and network services/applications resources/devices in all network segments.

Network 2030 is envisaged to support different and very stringent functional and non-functional requirements including the strict low latency and large volume of data exchange requirements. In some cases, these requirements are to be supported per network slice basis. Additional Network 2030 new composite characteristics and capabilities are:

- Enhancing IP best effort service provision with service quality information, network conditions enablers to achieve guarantees for KPIs or QoS as required by future precision services and applications per slice.
- Evolution towards native support network functions towards very low latency, very high bandwidth, very high reliability / resilience, trustworthiness and privacy, delivering stringent non-functional requirements with guarantees for KPIs / QoS per slice needed for future network service
- Determinism in Delays and Lossless Transmission

- Native support for multiple types of delivery services, in-time/on-time service activation and availability
- Elasticity in Network Services Customization and Network Functions Componentization
- Effective Programmable Network Protocol and Flexible Dynamic Transmission
- Intrinsic Secured Networking and Trust Networking
- Higher Levels of Robustness in face of failures
- Integration of large numbers on Intelligent methods (AI /ML based methods) in the Network Infrastructure, Control and Management
- Evolution towards intent driven distributed management of all physical and virtual network elements and network functions

A principle is a rule that governs how a system is to be realized; architectural principles are design choices used as a basis for the operation of the system. Each principle will apply to a particular set of viewpoints on the architecture. From the user point of view the principles of a system are understood as the essential characteristics of the system reflecting system's purpose and its effective operation.

The followings are proposed **Network 2030 specific architectural principle**s that are architectural primitives and key design choices.

The following picture depicts the relationships between Networ2030 principles, requirements and architecture(s).

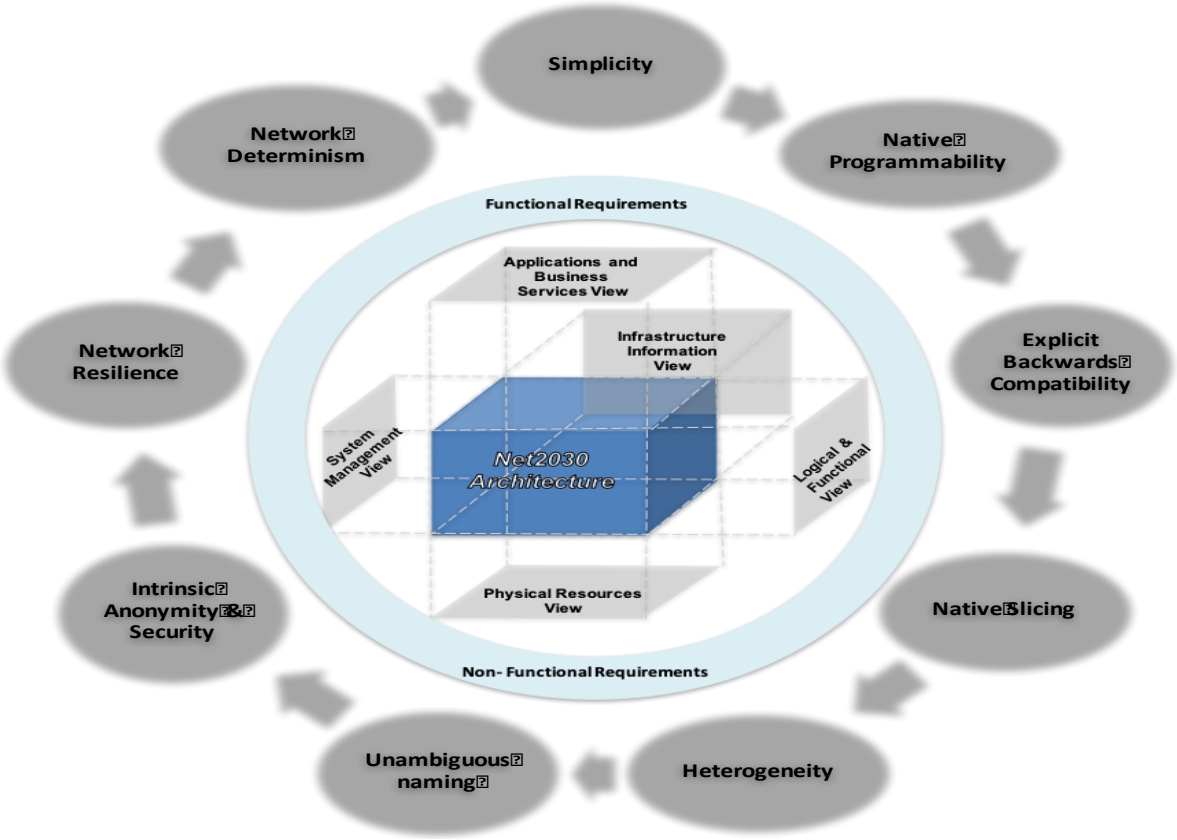


Figure 1 - Network 2030 Architecture Principles

8.1 Simplicity

Network 2030 represent a transition from monolithic network devices to virtualized network functions.

With the proliferation of virtualization, networks will consist of large number of virtualized and non-virtualized component which makes Network2030 complex. Complex systems are generally less reliable and less flexible. The Architectural Component Proportionality Law [RFC3439] states that the complexity / simplicity of an architecture is proportional/ invers proportional to its number of components. As such in order to increase the reliability or flexibility one way would be to reduce the number of components in a service delivery path (i.e. a service chain or a protocol path or a software/virtual path).

In large current interconnected networks, even small perturbations on the input to a process can destabilize or create a singularity in the system's output. As such complexity would significantly amplify small perturbations.

Thus, when architecting Network 2030, the famous indicator by Albert Einstein should be supported: "Make everything as simple as possible, but not simpler". In the current Internet, this principle was identified with the acronym KISS ("Keep it simple, Stupid!") [PRINCIPLE.1]

8.2 Native Programmability and Soft Re-architecting

Network 2030, architecture is expected to be extremely flexible and highly programmable with native softwarization infrastructures. As such Network 2030 represents an evolution of native flexibility and programmability conversion in all network segments.

In Network 2030, the decomposition of current monolithic network entities into network functions or network virtual functions would be necessary and these functions should be able to be composed in an “on-demand”, “on-the-fly” basis.

Programmability in Networks enables the functionality of some of their network elements to be dynamically changed. These networks aim to provide easy introduction of new network services by adding dynamic programmability to network devices such as routers, switches, and applications servers. Network Programmability empowers the fast, flexible, and dynamic deployment of new network functions and management services executed as groups of virtual machines in the data, control, management and service planes in all segments of the network infrastructure (i.e. wireless and wire access, core, edge and network cloud segments).

Programmability in Networks refers to executable code that is injected into the execution environments of network elements in order to create the new functionality at run time with the required security characteristics. The basic approach is to enable trusted third parties (end users, operators, and service providers) to inject application-specific services (in the form of code) into the network. Network services may utilize this network support in terms of optimized network resources and, as such, they are becoming network aware. The behavior of network resources can then be customized and changed through a standardized programming interface for network control, management, and servicing functionality.

In addition, Network 2030 shall empower service-network interaction by breaking the tight coupling between network and services and connect the network computing resources to form the cloud resource pools. In this way (1) different services can effectively programmatically call any network function component and/or resources on demand flexibly and quickly, based on the automatic allocation and elastic capacity expansion of the underlying network resources; (2) different users can choose network services and network function services according to their own needs.

The level of programmability in Networks should be articulated for any proposed Network 2030 architecture.

8.2 Backward Compatibility

Explicit compatibility is a very important practical principle. The followings are 3 important compatibility aspects.

A number of clean slate approaches or architecture have or are been proposed with significantly richer functionality than current Internet. It is impractical and enormously costly to deploy at large a new architecture if it does not inherently support existing network operation.

Network devices have a wide spectrum of capability. This span of capability is increasing due to the natural development of computers, and to the advent of IoT devices. IoT devices often have minimal hardware and compute resources, and hence have difficultly supporting classical network protocols. Network 2030 needs to capable of supporting, unifying and integrating protocols supporting differential services that optimally meet the needs of new micro (i.e. IoT devices) and new advanced devices, together with existing devices and to provide capabilities such as security, privacy and deterministic delay.

The Network 2030 needs to support the decoupling of services and network devices. This permits the service layer to flexibly use the underlying network resources according to need, and to dynamically schedule services amongst the available packet transport services and other resources.

The level of native and/or explicit backwards compatibility should be articulated and supported for any proposed Network 2030 architecture or transition towards an architecture.

8.3 Heterogeneity in communication, compute, storage, service and their integration

In the Network 2030, the heterogeneity is expected to be much higher and multi-dimensional than today. Multiple types of multiple network devices, network and /or service nodes, multiple protocols, multiple network and virtual network functions, multiple services, will exist.

Network infrastructures consist of fixed networks, mobile communication networks and other basic networks benefiting from key networking technologies such as Internet, Mobile Internet, Internet of Things, Cloud Computing, Big Data, and Satellite communications with the convergence of network and computing resources. Each network can become service provider delivering network capabilities, computing capabilities and data capabilities to meet the needs and requirements of services in the relevant industries.

As such that heterogeneity in communication, computation, storage and their integration should be supported in Network 2030.

8.4 Native Slicing

In today's Network, layering is good practice for both communication protocols and software implementations. This has led in some cases to faster deployments, but suboptimal solutions, especially in wireless communications where layering may be considered unsafe, as functions of each layer are carried out completely before the protocol data unit is passed to the next layer.

Network 2030 may introduce a concept of native slices for enabling easy and efficient execution of multiple and different types of Network 2030 services at a given time on the same infrastructure. A network slice is a set of network functions, infrastructure resources (i.e., connectivity, compute, and storage manageable resources) and service functions that have attributes specifically designed to meet the needs of a Network 2030 service. As such a network slice is a managed group of subsets of resources, network functions/network virtual functions at the data, control, management and service planes at any given time. Slices may offer single uniform capability interfaces to entities and network functions, abstracting the autonomous loosely coupled slice components with different functional and non-functional behavior.

The level of native slicing should be supported for any proposed Network 2030 architecture.

8.5 Unambiguous naming network functions and services

In today networks, the addressing of hosts must be the same at start and finish of transmission. In Network 2030, the network functions and services need to be unambiguous. The user or user systems are not accessing any more a specific server, but the content, function or service that the server would host. As such unambiguous naming/description of network functions, network virtual functions and services should be supported in Network 2030.

8.6 Intrinsic Anonymity and security support for all network operations

A failure of the network to deliver the required service due to a technical defect or as a result of an attack can have serious and/or widespread safety and economic consequences. Network 2030 must therefore be regarded as critical national infrastructure as far as national and global security and economy is concerned. In Network 2030 because of more stringent resilience requirements of future application scenarios involving communications with life and death impacts, including but not limited to transportation or medial control should not bear intermittent failures. Given the nature of the new services that will be deployed over Network 2030, the attack surface and nature of an attack will expand beyond the vulnerabilities of existing networks. The scope and means of protection are expected to require extension beyond the methods that networks currently use. Network 2030 must therefore be designed to be impervious to attack, and to contain any attack that breaks through the defenses so as to minimize its impact.

In Network 2030 anonymity represents the ability of the network to provide communications channels where one endpoint is not made aware of any identity of the other side of the communication. It supports for all network operations should be made inherent to all data (small and big data) and services. As such Network 2030 would incorporate two important aspects: (a) Anonymity of the network services offered and (b) Higher Protection of the infrastructure. This includes high degree of intrinsic anonymity (i.e. safeguard network operations from malicious attacks or from the collection of sensitive information by intermediaries), in time-sensitive and automation in all network operations.

With the increasing of mass terminals, virtualization of network functions, and diversification of applications, the network is becoming more open, with increasing exposed interfaces, more and more attacks and potential network threats. As such Network 2030 should consider security from the beginning of network architecture design to make security as key element of the new networking fabric. Such security fabric builds on an end-to-end security system including identity authentication, network security, platform security, data security and business security with guarantees for trustworthiness.

8.7 Resilience

Resilience needs to be an inherent property of Network 2030 networked systems; this means that resilience has to be designed as a primary principle of these networks and systems, explicitly extending the notion of network topology robustness that was introduced in the Internet.

In recent years, it has become evident that modern networked systems (and the services that they include and support) are critical infrastructures, because of the reliance that the users put on them. Not only that, if some of these systems fail to provide their expected service (there may be some ‘downtime’), then losses will occur in terms of time and money, and in extreme cases there may be damage and even loss of life. Critical infrastructures comprise of assets and systems that maintain societal functions, including health, safety, security, and the economic and social well-being of people. Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) are particular examples of critical infrastructures for the monitoring, control and automation of operational plants of various sorts, such as utility networks. SCADA systems monitor and control infrastructures including power plants, water utility, energy and gas pipelines, which makes them highly critical.

Providing protection in terms of security, safety and resilience in such networks and in Network 2030 is inherently considered to be of vital importance.

The sources of challenges for networked systems can include natural disasters such as flooding, weather events leading to failure of electrical power, over-demand for the services of the system, software bugs and consequent failures, hardware component faults, complexity leading to errors by a human operator, and cybersecurity attacks. Networked systems need to be able to continue to offer a satisfactory Quality of Service no matter what challenge they experience.

Resilience against attacks including control and management plane of networks needs to be stronger for 2030 network 2030 than for current networks because by running those critical services on top of them, these networks could become target for more and more adversaries.

8.8 Network Determinism

In order to meet end-to-end of new business applications such as industrial control, telemedicine, robotics and vehicle networking, Network 2030 needs to introduce explicit determinism in very stringent non-functional requirements with guarantees per partitions of the infrastructures. As such it provides a description of how well a network performs its functions and operations. Non-functional network requirements include accessibility, availability, certification, consistency, compliance, extensibility, fault tolerance, integrability, interoperability, maintainability, operability, performance, privacy, resilience, reliability, robustness, scalability, security.

Network 2030 must be designed on the basis that accurate clocks are available wherever they are needed to support the synchronization and scheduling of all network operations including the sending of packets. This is needed to support deterministic services and coordinated operation of both applications and the network itself.

Network 2030 needs to support lossless network transmission, in many scenarios, through dynamic virtual channel technology, push-pull hybrid scheduling mechanism and load balancing with packet-by-packet distribution mechanism, to meet the needs of zero packet loss, low latency and high throughput. As such Network 2030 needs to guarantee deterministic transmission quality according to specific application requirements.

Network Determinism should be supported in Network 2030.

9 Overall Architecture

9.1 Introduction

Network2030 requirements, capabilities and services to be support are described in FG-NET2030 Sub-Group 1 and 2 specifications [Sub-Group 1.1, Sub-Group 2.1, Sub-Group 2.2]. Furthermore, future network requirements and architecture are described in [ITU-T.1, ITU-T.2]. The intent of this specification is to define an architecture to satisfy these requirements and support services that are expected to emerge in the coming decade.

As described in our principles in Section 2, Network2030 architecture is an end-to-end integrated, automated and dynamic architecture that combines connectivity, applications, and computation and storage resources. This architecture, that represents a transition from the current architecture of pure connectivity, is driven from proliferation of virtualization, Artificial Intelligence (AI)/ Machine Learning techniques, APIs for automation, optical computing, and current and expected future applications requiring enormous bandwidth, the end-to-end delay of a couple miliseconds, and near zero packet loss.

Applications for Network2030 are expected to be used by various end devices including robots, self-driven cars, and drones as depicted in **Figure 2**.

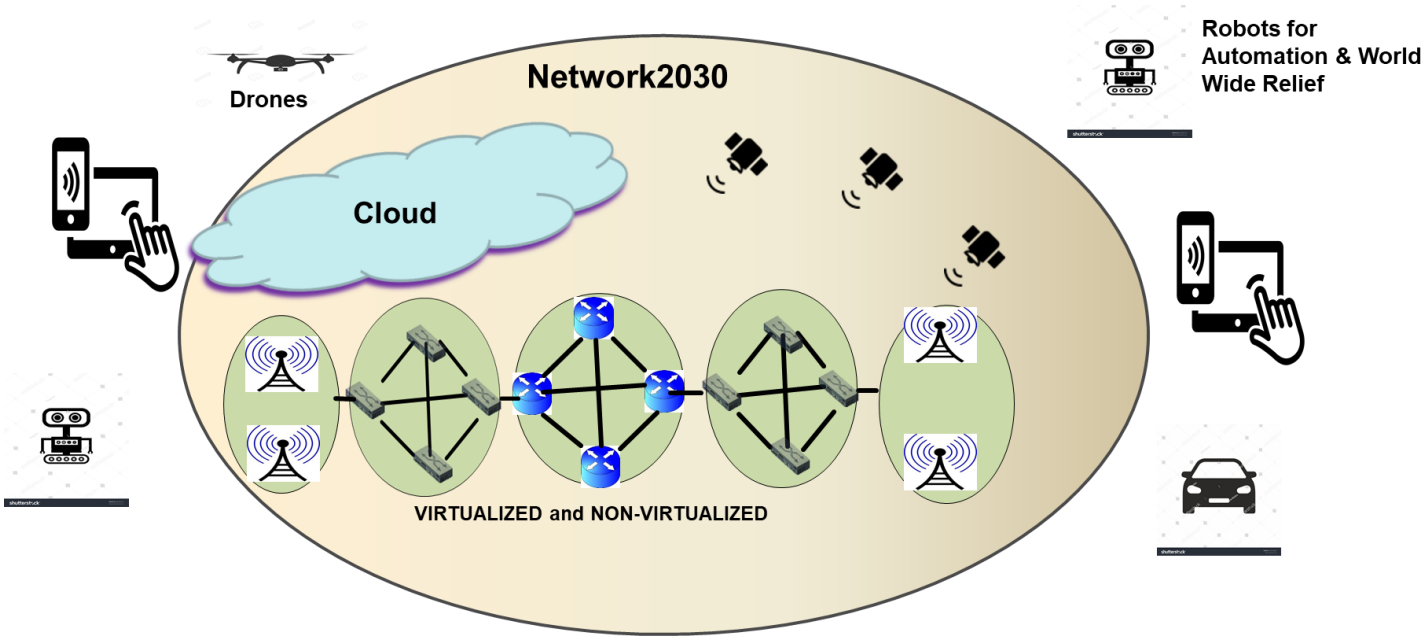


Figure 2 – An example of future network infrastructure and end devices

In order to support various applications driven by devices in **Figure 2** and devices to be developed in the future, the Network2030 infrastructure is expected to include fixed and wireless networks, cloud and space communications infrastructures as depicted in **Figure 3**. We expect virtualization, memory and computing technologies in addition to Artificial Intelligence (AI)/ Machine Learning (ML) continue to impact Network2030.

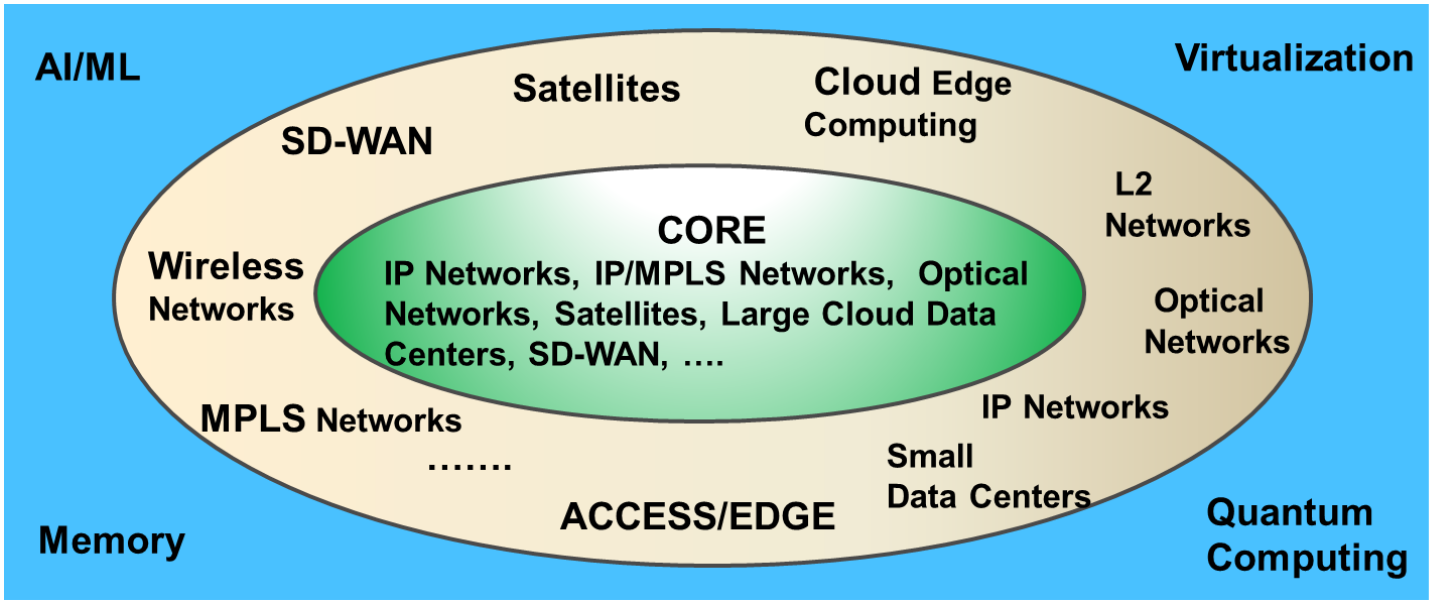


Figure 3 –Expected Network2030 Infrastructure

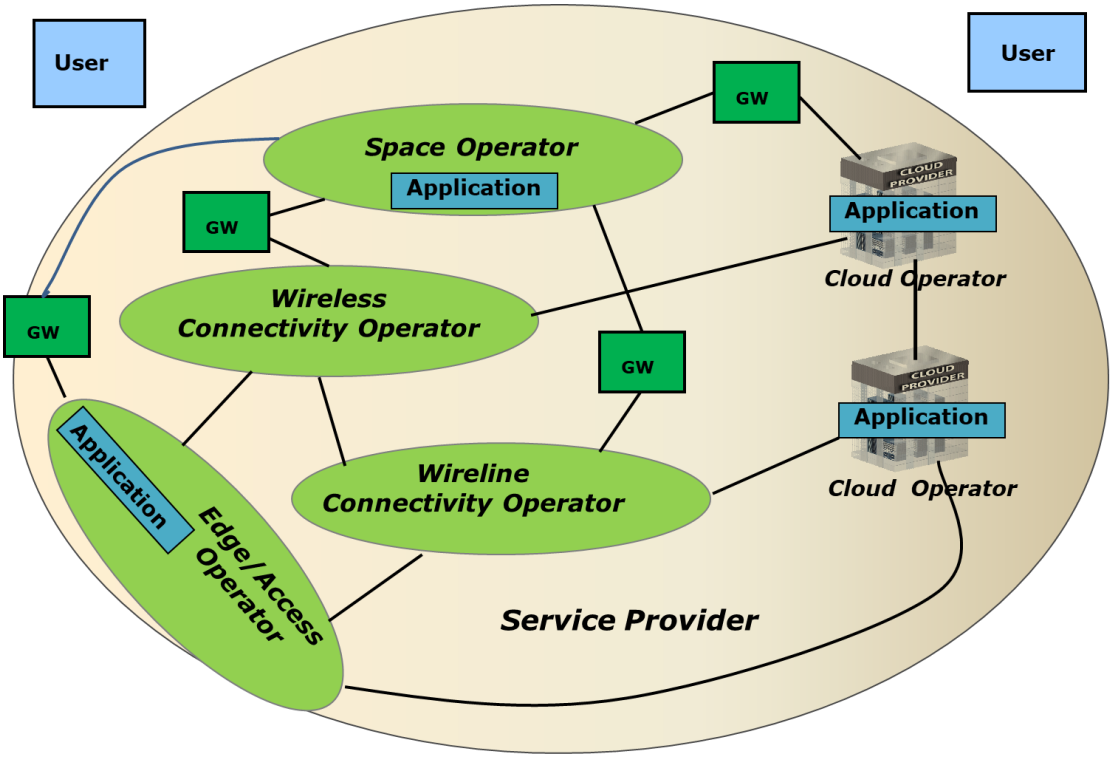
The following sections describe Network2030 Architecture components.

9.2 Network2030 Architecture

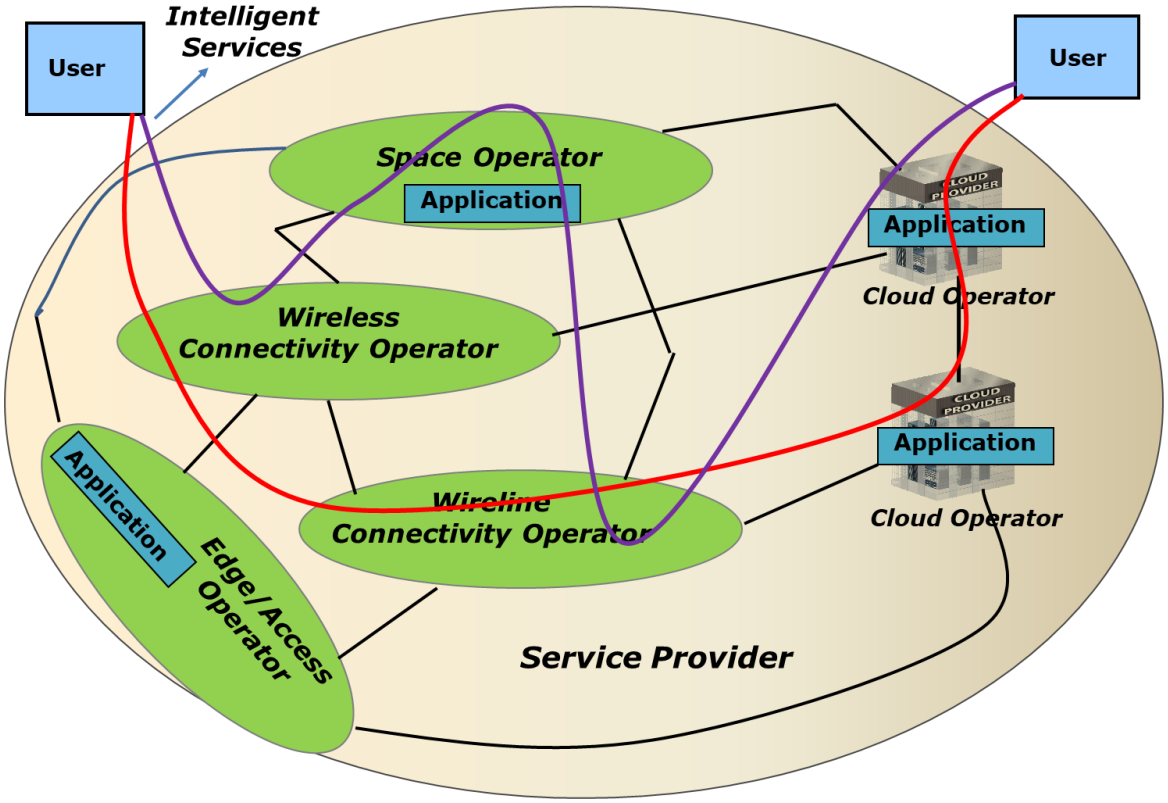
Key actors of Network2030 as depicted in **Figure 4** are:

- User: A person or organization or a machine that maintains a business relationship with and uses service from a Service Provider, or just uses the public network for connectivity between his/her and its application.
- Connectivity Operator: An intermediary that provides connectivity between Cloud Operators, Connectivity Operators, and users. In case of Internet, the Connectivity Operator is a public network provider.
- Space Operator: An Operator that may provide connectivity as well applications in the space.
- Edge/Access Operator: An operator that provides edge computing and/or access networking.
- Cloud Operator: An entity that is responsible for making applications available to users. It can be public or private.
- Service Provider (SP): An entity that is responsible for the creation, delivery and billing of services, and negotiates relationships among Cloud Operators, Connectivity Operators, Space Operators, and Users. It is the single point of contact for the user.

Today, a service provider which is responsible from a service over Internet end-to-end does not exist. Whether Internet Service Providers (ISPs) will act as a service provider by 2030 or not remains to be seen. However, this concept will allow us to define relationships among entities involved in providing an Internet service and automate the processes to support best effort as well as high quality services for a user dynamically without coordination among Internet providers in advance. The services supported by Network2030 are called as Intelligent Services due to their expected end-to-end automation and dynamicity.


User
User
GW
Space Operator
Application
GW
Application
Cloud Operator
Wireless
Connectivity Operator
GW
GW
Application
Application
Edge/Access
Operator
Wireline
Connectivity Operator
Cloud Operator
Service Provider

(a) Actors



(b) Intelligent Services

Figure 4 – Actors of Network2030 and Intelligent Services among them

9.2.1 Characteristics of Network2030

Network2030 includes connectivity and application functionalities with greater flexibility and automation in service order, provisioning, monitoring and billing. Some of its characteristics are [ARCH.1, ARCH.2]:

- consisting of virtualized components (VNFs-Virtual Network Functions) and non-virtualized components (PNFs-Physical Network Functions);
- consisting of network functions with just non-virtualized components (PNFs) or both virtualized components (VNFs) and non-virtualized components (PNFs);
- consisting of applications built with virtualized components (VNFs);
- consisting of connections provided by one or more Public Cloud Provider (s), Private Cloud Provider (s), Fixed and Wireless Network Operator (s), Edge/Access Operators, and Space Network Operator (s);
- consisting of applications provided by one or more Cloud Providers, Space Operators, and Edge/Access Operators;
- supporting best effort as well as highly available (i.e. higher than 5 of 9 availability) and high precision services requiring bandwidth from Gbps to Tbps;
- supporting elasticity for dynamic service configurations by users, and locations of the service functionality;
- supporting service monitoring and usage-tracking by users;
- supporting programmability, self-service by users, and collaboration among Operators;
- supporting scalability of resources dynamically;

- supporting various high availability options from physical layer to application layer; and
- supporting "pay as you use" (i.e. usage based billing).

It is expected that Network2030 Service Providers strike a balance among programmability, self-service by users and the Service Provider control of resources to ensure integrity, security, and availability of Network2030. Service Providers may need to place appropriate controls for the self-service and programmability to avoid possible unintended failures.

9.2.2 Interfaces

A user interfaces to a Service Provider's facilities via **a User Interface** consisting of Connectivity UNI and Application UNI [ARCH.3], as depicted in **Figures 5** and **6** which are implemented over a bidirectional link that provides various data, control and management capabilities required by the Service Provider to clearly demarcate two different connectivity domains and two different application domains involved in the operational, administrative, maintenance and provisioning aspects of the service. The Application UNI may not exist at the User Interface when only connectivity services are offered at this interface (**Figure 7**).

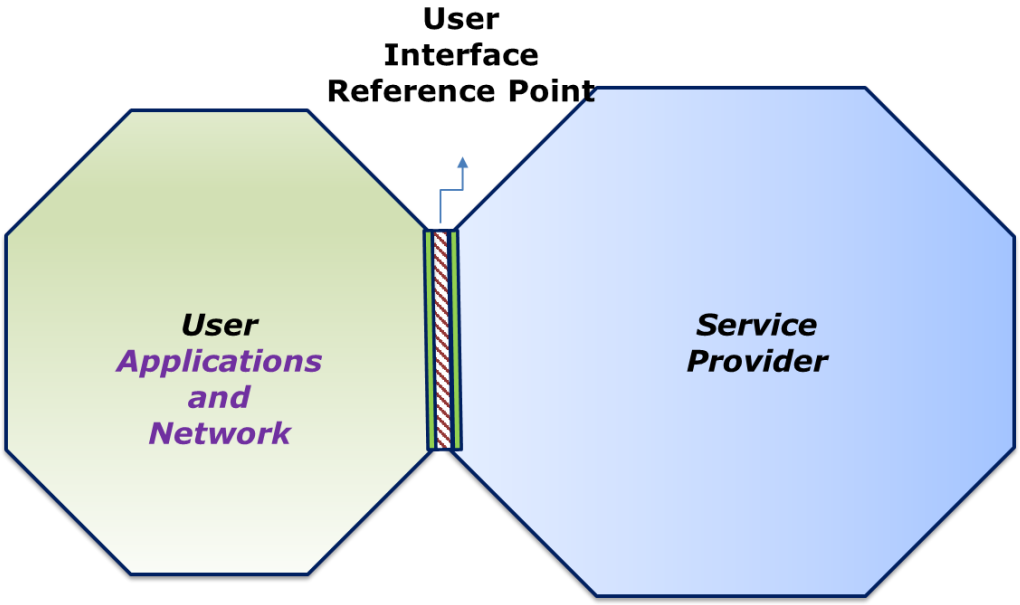


Figure 5- User Interface

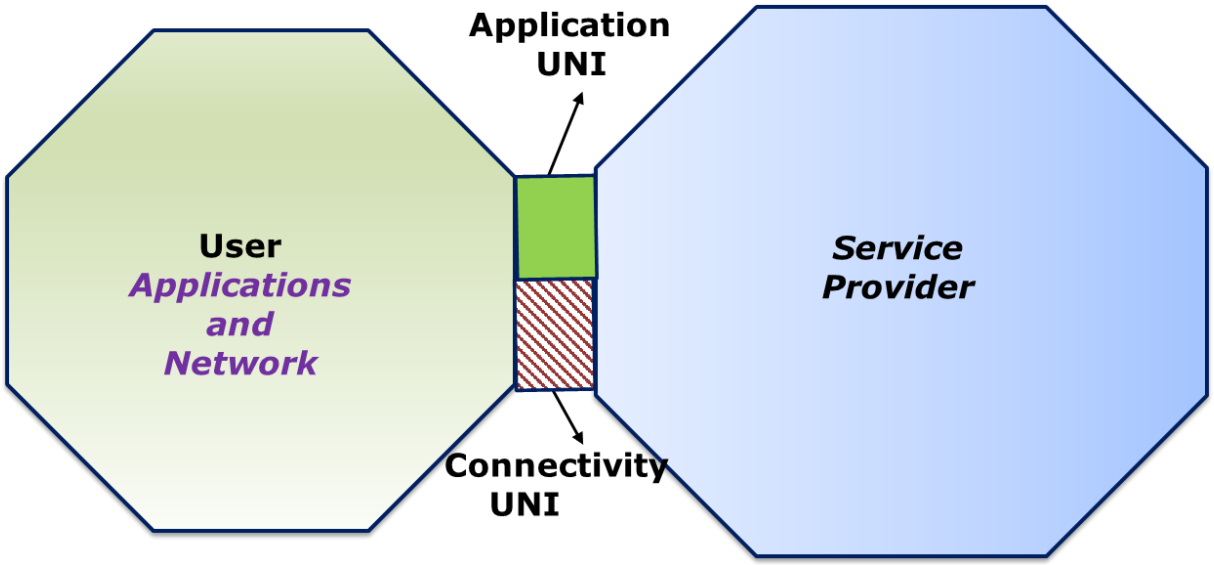


Figure 6- Connectivity UNI and Application UNI between User and SP

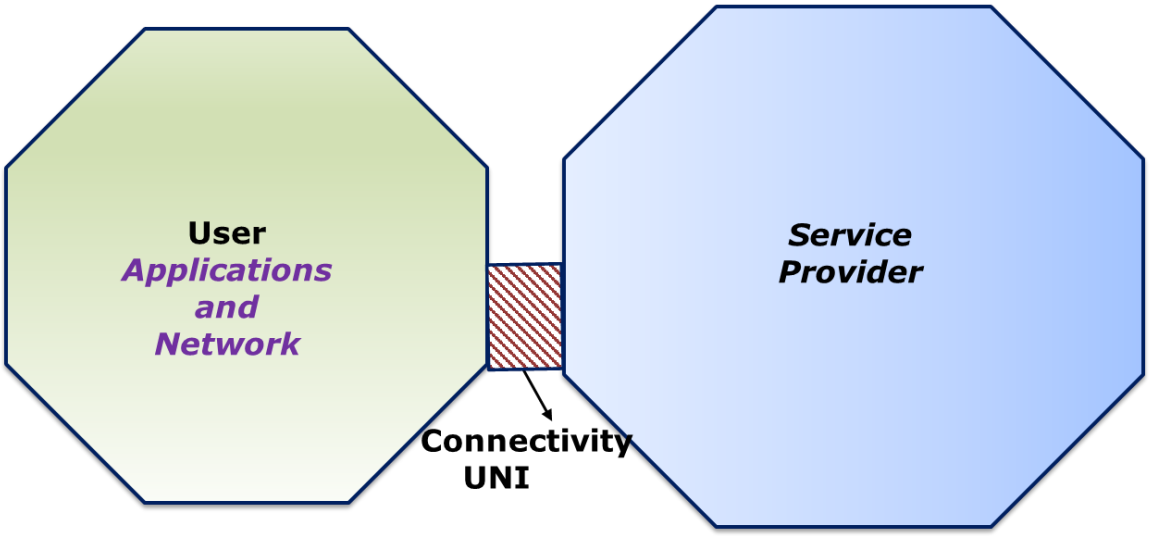


Figure 7 – User Interface consisting of only Connectivity UNI

The protocol stack for the User Interface is depicted in **Figure 8**. Depending on the service offering, the protocol stack for Connectivity UNI can be Layer 1, Layer 2 or Layer 3 (**Figure 9**). For example, Connectivity UNI is an Layer 2 interface for Carrier Ethernet Services and an Layer 3 interface for IP services.

Depending on the service offering, the protocol stack for Application UNI can be Layer 2 and above (**Figure 9**).

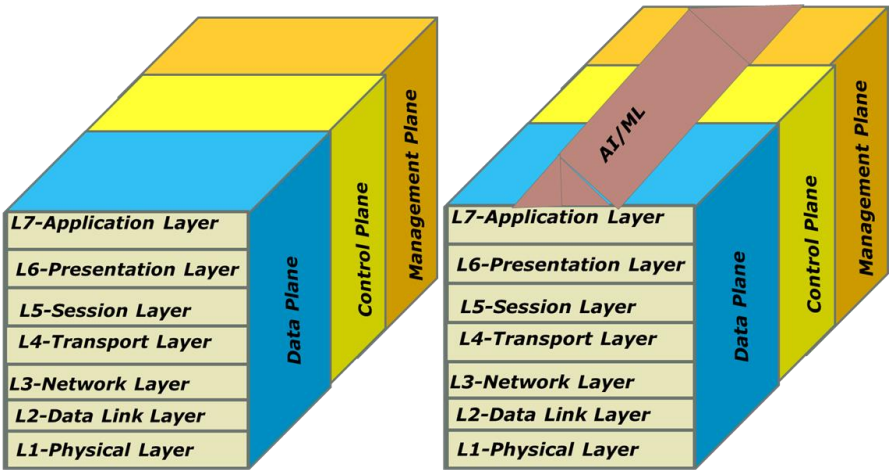
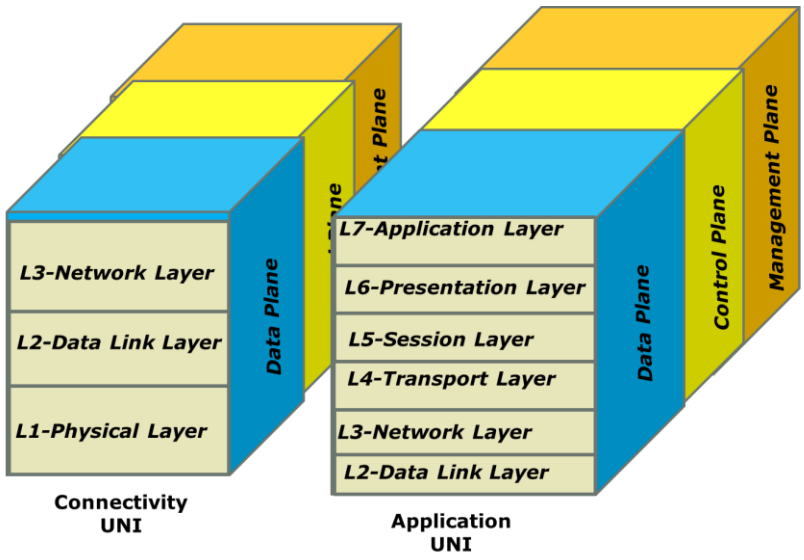
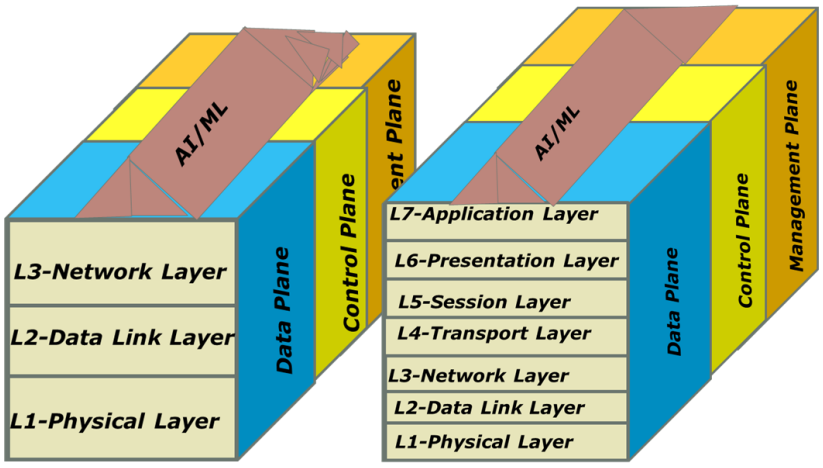


Figure 8 – User Interface Protocol Stack with and without AI/ML Functionalities



(a) Connectivity UNI and Application UNI without AI/ML



(b) Connectivity UNI and Application UNI with AI/ML

Figure 9 –Connectivity UNI and Application UNI Protocol Stacks

In all layers of interfaces depicted in **Figures 8** and **9**, we expect to see AI/ML as a common capability.

Figures 5-9 describe an interface between a User and a Service Provider. Although there is no Service Provider for services provided over Internet, we still expect to use this standard interface for services provided over Internet. It is clear that attributes for the User Interface will be different for different connectivity layer and application layer, to be standardized by the industry.

Similar to the protocol stack, attributes of the User Interface are expected to vary from one service to another. They are expected to be defined and standardized in parallel to the evolution of Network2030.

Some of the attributes of the User Interface are described in [ARCH.7]:

- Physical layer attributes such as the attributes of Ethernet;
- Connectivity attributes such as number of V-LANs and Ethernet Virtual Connections supported;
- Application attributes such as Virtual Machine (VM) and Virtual Network Function (VNF) attributes;
- Traffic management attributes such as bandwidth;
- Resiliency attributes such as access link redundancy;
- Fault management attributes such as alarms/events associated with the User Interface failures;
- Performance management attributes associated with measurements at the interface;
- Security attributes for securing User access to Network2030 services; and
- Billing attributes

These attributes can be grouped into Connectivity UNI and Application UNI.

In providing services to a user, two Operators interface each other via an Operator-Operator Interface [ARCH.3] as depicted in **Figure 10**. Operator-Operator Interface is defined as a reference point representing the boundary between two Operators that are operated as separate administrative do-mains. This reference point provides demarcation between two Operators for services.

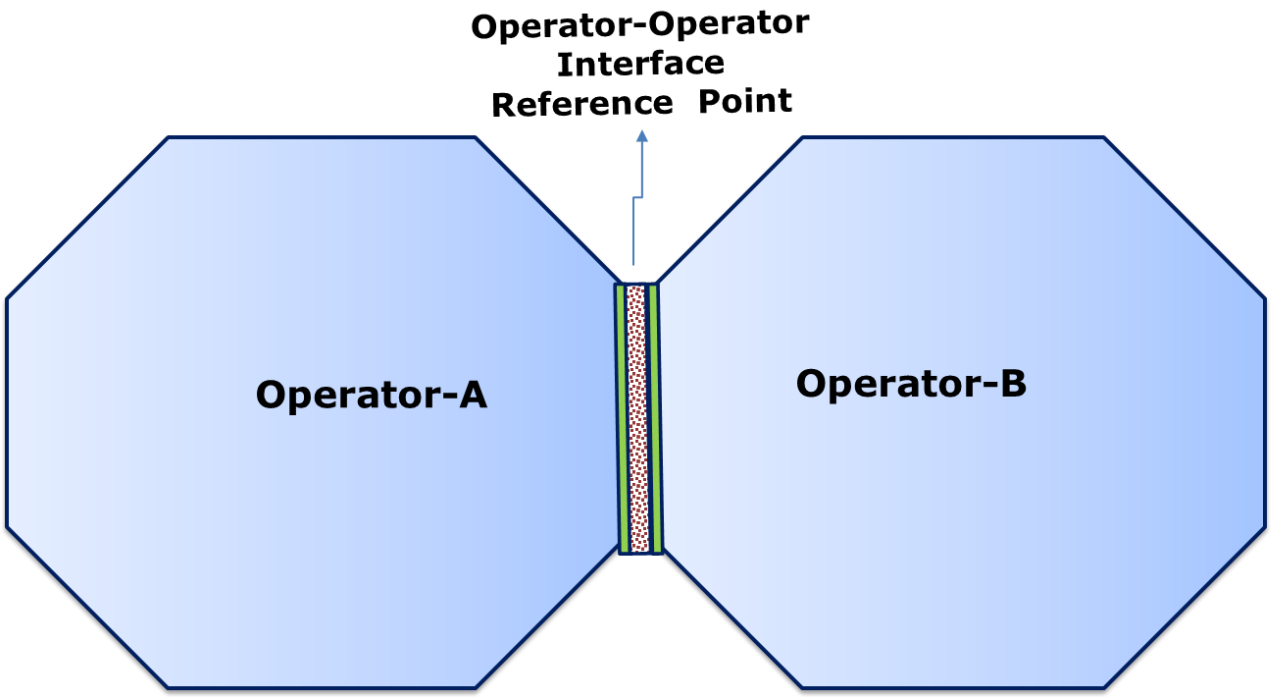


Figure 10 – Two Operators interfacing each other via Operator-Operator Interface

Operator-Operator Interface consisting of Connectivity ENNI and Application ENNI as illustrated in **Figure 11**. The Application ENNI may not exist at the Operator-Operator Interface when only connectivity services are offered at this interface (**Figure 12**).

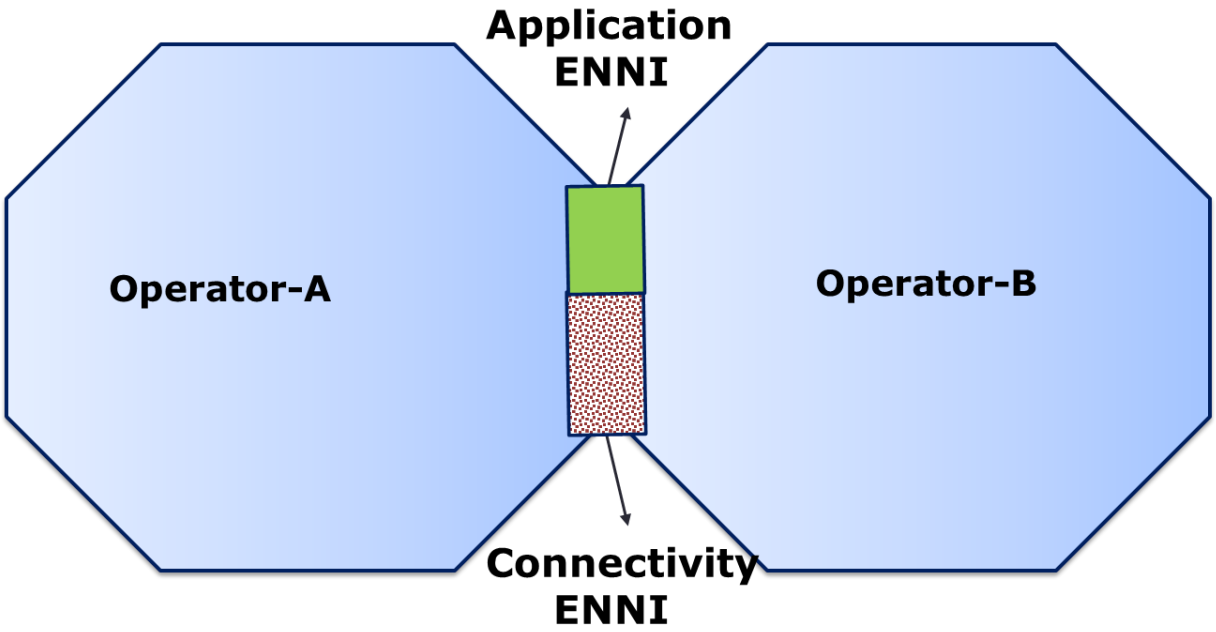


Figure 11 –Connectivity ENNI and Application ENNI between two Operators.

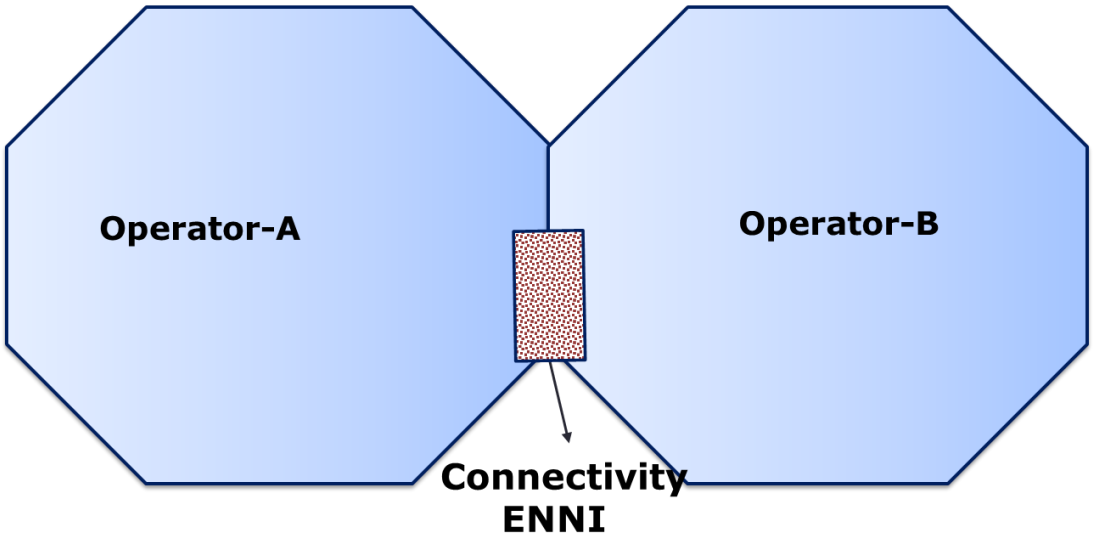


Figure 12 –Operator-Operator Interface consisting of only Connectivity ENNI

Operator-Operator Interface protocol stack is the same as the protocol stack for the User Interface in **Figure 8**. Similarly, the protocol stacks for Connectivity ENNI and Application ENNI are the same as those for Connectivity UNI and Application UNI in **Figure 9**, respectively.

Depending on the service offering, the protocol stack for Connectivity ENNI can be Layer 1, Layer 2 or Layer 3. Similarly, the protocol stack for Application ENNI can be Layer 2 and above, depending on the service offering.

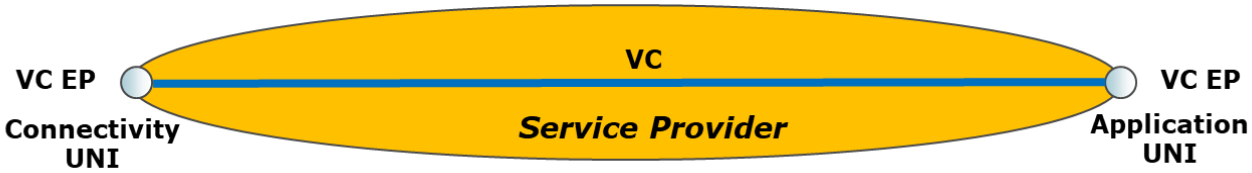
Some of the attributes of the Operator-Operator Interface are described in [ARCH.7] as well. These attributes can be categorized similar to those for the User Interface, and grouped into Connectivity ENNI and Application ENNI.

Both protocol stack and attributes of the Operator-Operator Interface are expected to vary from one service to another. They are expected to be defined and standardized in parallel to the evolution of Network2030.

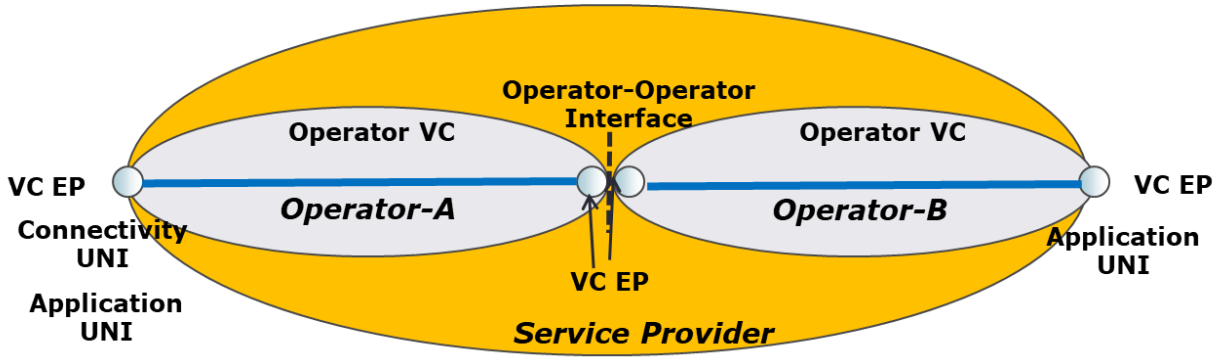
9.2.3 Connections and Connection End Points

Connection and connection end points [ARCH.1, ARCH.2, ARCH.3] providing services are depicted in **Figure 13** for a Virtual Connection (VC) crossing one or more administrative domains.

When a VC crosses multiple Operators, the VC segments and their end points in each Operator are called Operator VC and Operator VC End Point (Operator VC EP), respectively.



(a) VC between two end points residing on the resources of an Operator which is a SP.



(b) VC between two end points residing on the resources of two different Operators.

Figure 13- Virtual Connection and its Segments

The VC EP is an end point of a VC when the VC is within the boundaries of one administrative domain. User Interface identifier, availability, bandwidth profile, parameters of security functionalities, administrative state and operational state are among the attributes of VC EP.

The VC is an association of two or more VC EPs. The VC could be an Ethernet Virtual Connection (EVC), Label Switched Path (LSP), IP VPN or SD-WAN connection. Identifiers of VC EPs associated with this VC, connection type, Service Level Specification (SLS), redundancy, connection start time, connection duration, connection period, billing options, Maximum Transmission Unit (MTU) which is the maximum size of Service Protocol Data Units (PDUs) transmitted over the VC, administrative and operational states are among the attributes of VC.

The VC EP is a logical end point of a VC where the VC is terminated at a UNI, ENNI or Application Interface (i.e. Application UNI or Application ENNI), to which a particular set of Service PDUs that traverse the UNI, ENNI or Application Interface is mapped. As an example, the particular set could be identified by attributes such as application identifier, source and/or destination IP address, C-Tag VLAN ID, etc., depending on the Service PDU.

Service PDUs transported over a VC in both ingress and egress direction are tracked at UNIs and ENNIs to ensure alignment with Service Level Objectives (SLOs) and identify possible service problems.

The VC may cross multiple Operator domains as depicted in **Figures 14** and **15**. Each domain will carry a segment of the VC. The segment in each Operator domains is called Operator VC.

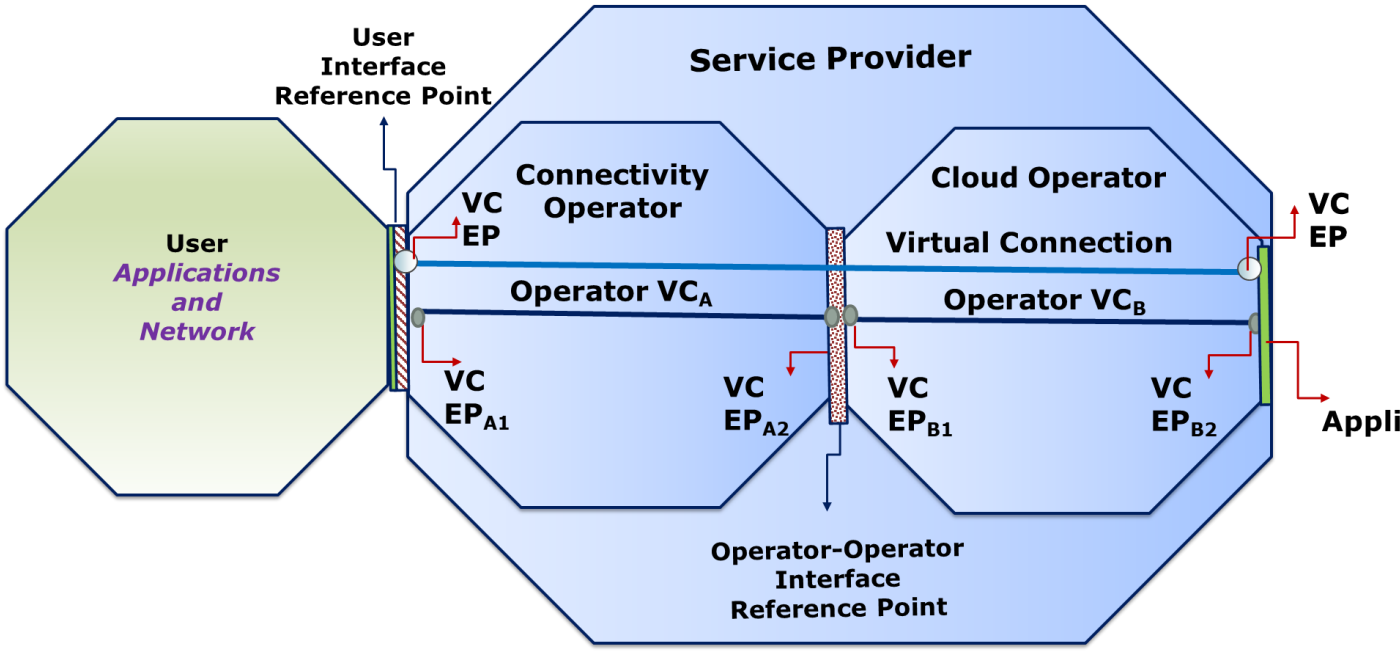


Figure 14- Virtual Connection crossing Two Operators

An example service architecture is depicted in **Figure 15** where two Operators provide connectivity and applications while one Operator provides just connectivity. The cloud applications form service function chaining (SFC).

In this figure, Operator-A could be a private network Operator acting as the Service Provider in addition to providing connectivity as the Connectivity Operator, Operator-B could be a Public Cloud Provider, and Operator-C could be a Space Operator.

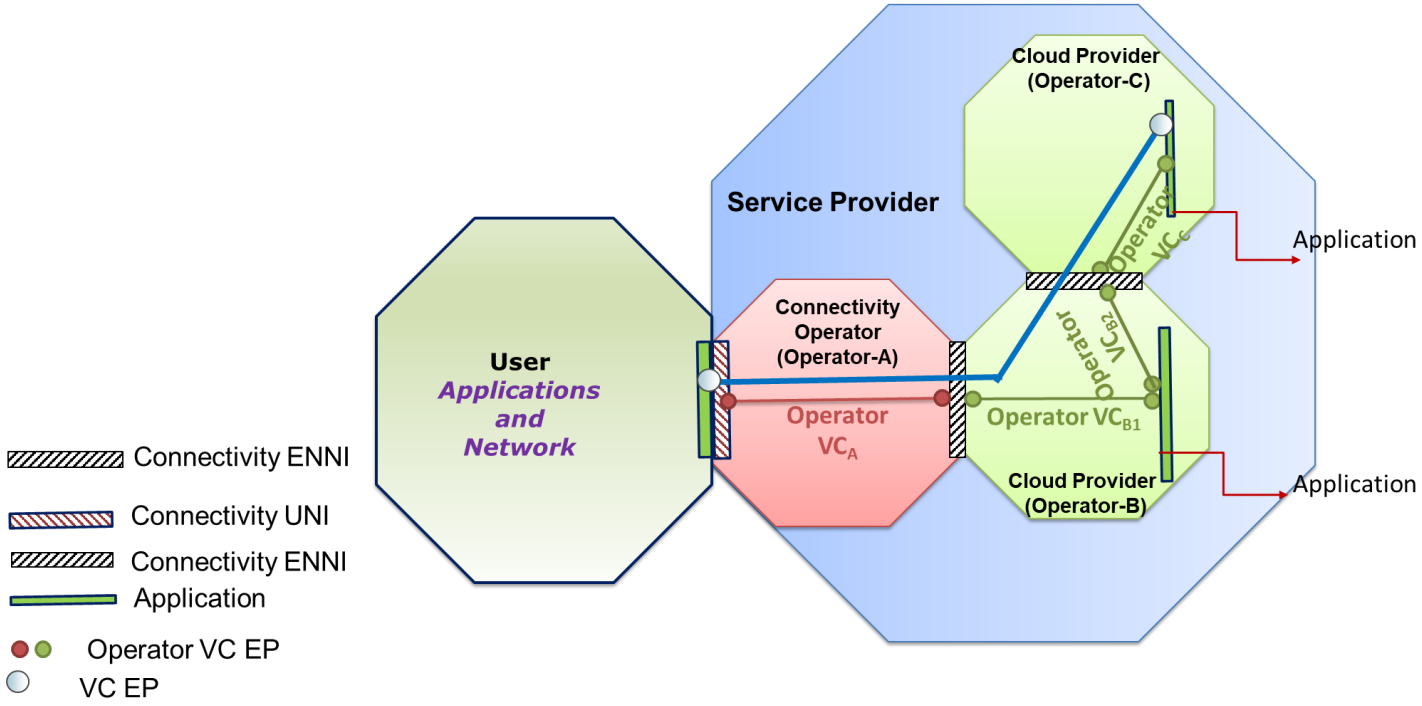


Figure 15- A Service Configuration

In order to establish a SFC between two VNFs, each VNF needs to support a standard Application Interface depicted in **Figure 9.**

9.3 **Management Architecture for Network2030**

High level Network203 architecture and its characteristics are described in Section 9.1. Emerging applications and services that Network 2030 needs to support are described in [Sub-Group1.1]. Some of the key services that are expected to have substantial impact on Network2030 are:

- In-time and on-time services such as manufacturing automation, remote surgery, and Haptic communications;
- Tightly coordinated services such as self-driven cars; and
- High throughput multimedia services such as those supporting Holographic applications.

These services have the following characteristics:

- High Precision that requires to meet stringent Service Level Objectives (SLOs). These objectives must be met.
- No Graceful Degradation: Traditional network services degrade gracefully when service levels deteriorate. For example, when latency and/or jitter increase gradually or slightly, the Quality of Experience will be negatively affected and decrease by some degree – for example, video resolution of color depth of video may be reduced or drops in Mean Opinion Scores may be observed. However, even in the presence of slight deterioration, the service as a whole and applications relying on it will still fundamentally be usable. In contrast, Network 2030 services may not degrade gracefully; instead, even a slight deterioration may rapidly lead to a complete breakdown of the Quality of Experience which renders associated applications unusable. An example concerns haptic communications services, where extended latency may result in a loss of the illusion of haptic control needed to operate remote machinery confidently.
- Mission Criticality: Some of Network2030 services are for mission-critical services for which occasional failure is not an option. For example, loss of control when operating remote machinery may result in risks for public safety. This implies that 5 of 9 availability for most of Network2030 services is inadequate.
- High Accuracy Measurements: High Precision service level requirements impose the need to be able to measure those service levels with high accuracy and in real-time. For example, delay and jitter may need to be measured with microseconds or fraction of miliseconds granularity, although clock synchronization is expected to be challenging.
- Tamper Proof Service Level Validation: The mission criticality and lack of graceful degradation of associated services implies that such services will be under increased scrutiny and potentially subject to regulation and litigation. This will require validation of service levels and proof of delivery according to service level objectives in ways that are trusted and tamperproof, i.e., whose correctness can be independently verified and whose records will potentially hold up also in the case of litigation. Therefore, service assurance will not be able to rely as much on statistical sampling as in the past. Instead, coverage and assurance of each service instance must be provided throughout the duration or lifetime of the service instance.

With the Network2030 architectural constructs (i.e. interfaces, connection and connection end points) that are described in the previous section, current and emerging services are expected to be modeled by identifying service specific attributes and managed accordingly.

The following management functions need to be performed end-to-end for a service over Network2030:

- **Order Fulfillment and Service Control** [ARCH.4, ARCH.5] that support the orchestration of provisioning related activities for the fulfillment of a Customer order or a Service Control request, including the tracking and reporting of the provisioning progress. In Network2030, we expect these functions are to be performed dynamically with a performance that is acceptable to end users. These functions can be grouped as:
    - **Order Fulfillment Orchestration** that involves in decomposing a customer order into one or multiple service provisioning activities and orchestrating of all customer order-related fulfillment activities;
    - **Service Configuration Orchestration** which is responsible for the design, assignment, and activation activities for the end-to-end service and/or some or all service components;
    - **Service Control Orchestration** that permits the service to be dynamically changed within specific bounds described in policies that are established in advance or created on the fly with the Intent Based Networking (Section 17.6) approach;
    - **Service Delivery Orchestration** which is responsible for the service delivery via network and application implementation delegation of each service component to their respective delivery system or mechanism; and
    - **Service Activation Testing Orchestration** that coordinates all service activation testing activities, for parts and/or the complete end-to-end service. The testing can be performed by Service Provider as well as by User.
- **End-to-End Service Testing Orchestration** which is automating all test functions such as Service Activation Testing and In-Service Testing, and verification of services, seamlessly, across multiple operators.

  The end –to-end service testing orchestration may require orchestration and control of the different systems capable of conducting tests and reporting on services that may be implemented within the infrastructure, the element control managers or can be deployed on demand, in the form of virtual machines.

  As the different locations and Network2030 elements involved in the fulfillment of end-to-end services may not all be available at the same time, the Service Testing Orchestration flexibility allows for real-time staggered testing, from simple unit level connectivity tests, to end-to-end comprehensive Service Activation Testing.

  Customer acceptance is received from the Customer. The Customer may view their particular services test results, or under special agreement with their Service Provider, be able to perform a set of predefined service acceptance tests.
- **Service Problem Management** which is alarm surveillance, including the detection of errors and faults related to service, either end-to-end or per service component, and fixing failures automatically. In Networ2030, we expect self-managed networks and services [ARCH.6] to be implemented using Artificial Intelligence and Machine Learning techniques as described in Section 11.6.

  Customers are able to track the service impact of failures and status of trouble resolution.

- **Service Quality Management** includes the collection of service performance information (e.g., delay, loss, availability, etc.) in support of key quality indicators across all Operators depicted in **Figure 4** who participate in delivering the service. This also includes gathering of feedback from the Customer, including Customer-provided performance measurements. Service quality is analyzed by comparing the service performance metrics with the service quality objectives described in the Service Level Agreement (SLA) between Customer and Service Provider. The results of the service quality analysis are provided to the Customer as well as information about known events that may impact the overall service quality (e.g., maintenance events, congestion, relevant known problems, demand peaks, etc.). Service Quality Management capabilities also include capacity analysis in support of traffic engineering, traffic management, and service quality improvement.

  As new applications and verticals with new business models requiring high precision appear in Network2030, verification of delivered service levels will become important to billing and charging.

- **Billing and Usage Measurement** capabilities enable operators to gather and provide usage measurements, traffic measurements, and service-related usage events (e.g., changes in service bandwidth, etc.) describing the usage of service components and associated resources. Exception reports may be generated to describe where service components and resources have been used beyond the usage commitments as described in the SLO.

- **Security Management** provides for the protection of management and control mechanisms, controlled access to the network and applications, and controlled access to service-related traffic that flows across the network and applications within and across Operators. Such security management capabilities support the authentication of users and applications and provide access control to the variety of capabilities on Application Programming Interfaces (APIs) supporting management and control based on the roles assigned to each authorized user. The security management capabilities include encryption and key management to ensure that only authenticated users are allowed to successfully access the management and control entities and functions; and preventing unauthorized modification/deletion of data . The security management takes responsive steps, such as applying filtering controls on specified traffic flows, when a specific threat and attack for Network 2030 is identified.

  The Security Management also provides audit trails for communications or ensure communications does not cross certain geographical boundaries.

  Details of Security and Privacy capabilities are addressed in Section 13.

- **Analytics** capabilities are for supporting the fusion and analysis of information among management and control functionality across management domains in order to assemble a relevant and complete operational picture of the end-to-end services, service components, and the supporting network and application infrastructure – both physical and virtual. Analytics ensures that information is visible, accessible, and understandable when needed and where needed to accelerate decision-making. For example, the analytics may utilize service fulfillment, control, and usage information to predict and trend service growth for the Connectivity and Cloud Operators. Section 5.4 discusses analytics application at the Edge.

- **Policy Based Management** is the prescribing the management behavior by a set of rules under which the orchestration, management and control logic operate. Service policies may be encoded in such rules in order to describe and design the dynamic behavior of services. Coordinated service relies on the orchestration of distributed capabilities across potentially Operators to enable end-to-end management. The policy-based management capabilities provide rules-based

coordination and automation of management processes across administrative domains supporting effective configuration, assurance, and control of services and their supporting resources.

Service design policies may enable the design and creation of end-to-end automated services. Service objectives may be implemented as sets of policies with event-triggered conditions and associated actions, as well as intent-based policies. Such policies would adjust the behavior of services and service resources – including bandwidth, traffic priority, and traffic admission controls – allowing Services to adapt rapidly to dynamic conditions in order to satisfy critical, ever-changing needs and priorities.

Policy based management may use Intent-based Networking (IBN) and Artificial Intelligence (AI)/Machine Learning (ML) techniques that are described in Section 17.

- **Customer Management** involves in Service Provider interaction with potential Customers to determine serviceability of a Product Offering and if the underlying infrastructure is both capable and available to support the desired service for the Customer. In Network2030, we expect that Network Slices and services on a Network Slice are to be requested dynamically from Service Provider via Customer Network Management.
- **Partner Management** involves in Service Provider interaction with Partners to determine service feasibility. For certain services such as those related to Internet of Things (IoT), it is likely to have service run-time interactions between SP and Partner.

Network2030 needs a management architecture that can support the functionalities described above for services running over it without manual intervention dynamically. Given there is no Service Provider responsible for the end-to-end management of a service over Internet, the user and/or ISP is responsible for the end-to-end service life cycle management. This can be accomplished if all the processes associated with service life cycle management is automated even if the service is supported by multiple Operators.

A high level management architecture is depicted in **Figure 16** and **Figure 17**, where each Operator providing a segment of Network2030 assigns an Orchestrator and Operation Support Systems (OSS)/Billing Support Systems (BSS) to manage all the resources and associated services in its domain and interoperate with Orchestrators and OSS/BSS of other Operators involved in the same service. The user is allowed to interact with the Orchestrator and OSS/BSS of his/her Internet Provider (ISP) as in the Lifecycle Service Orchestration (LSO) architecture in **Figure 17**.

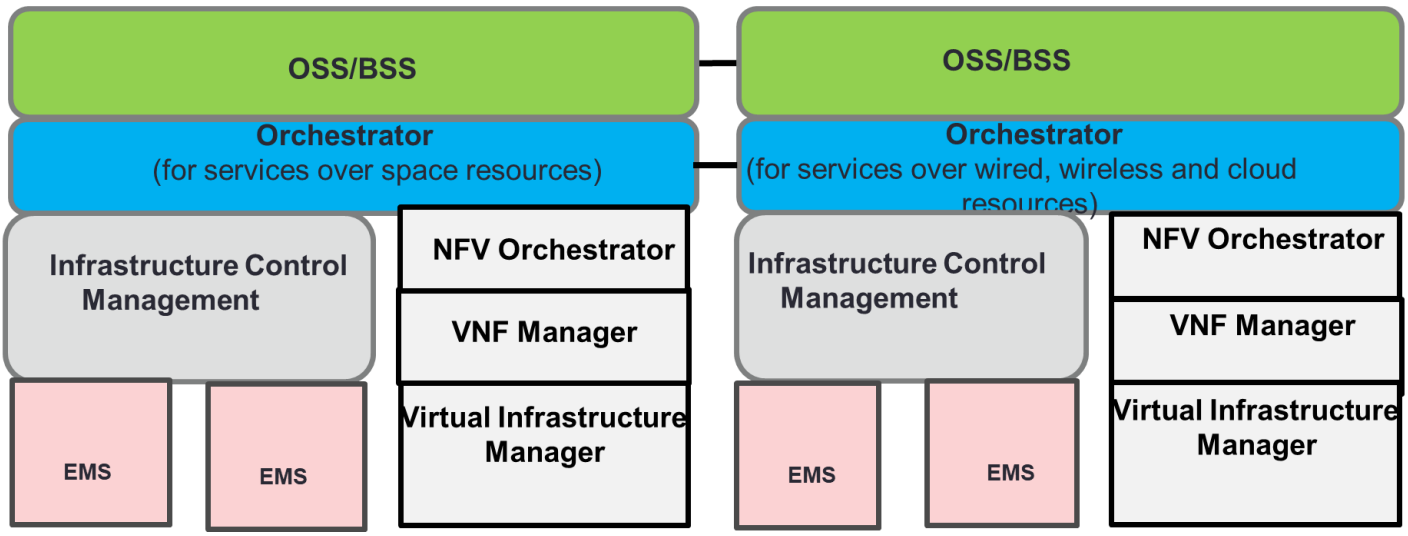
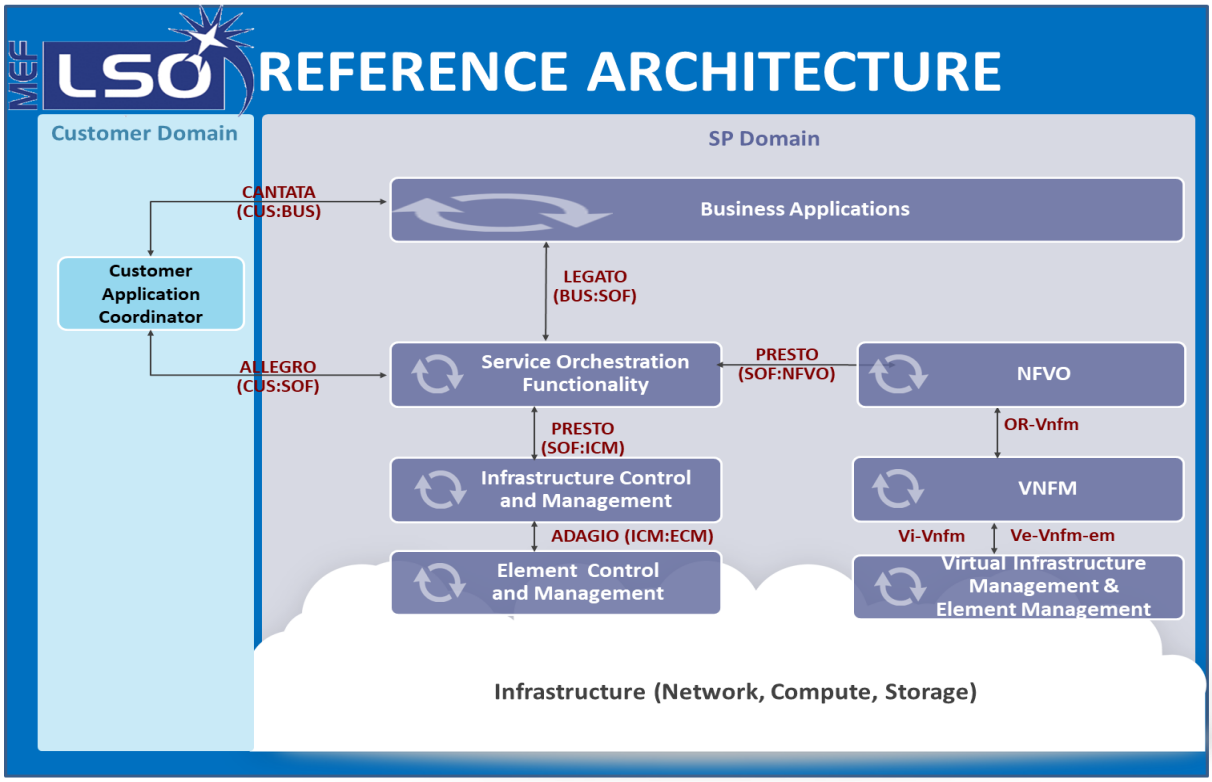


Figure 16- End-to-end Orchestration of Network2030 and Services over it

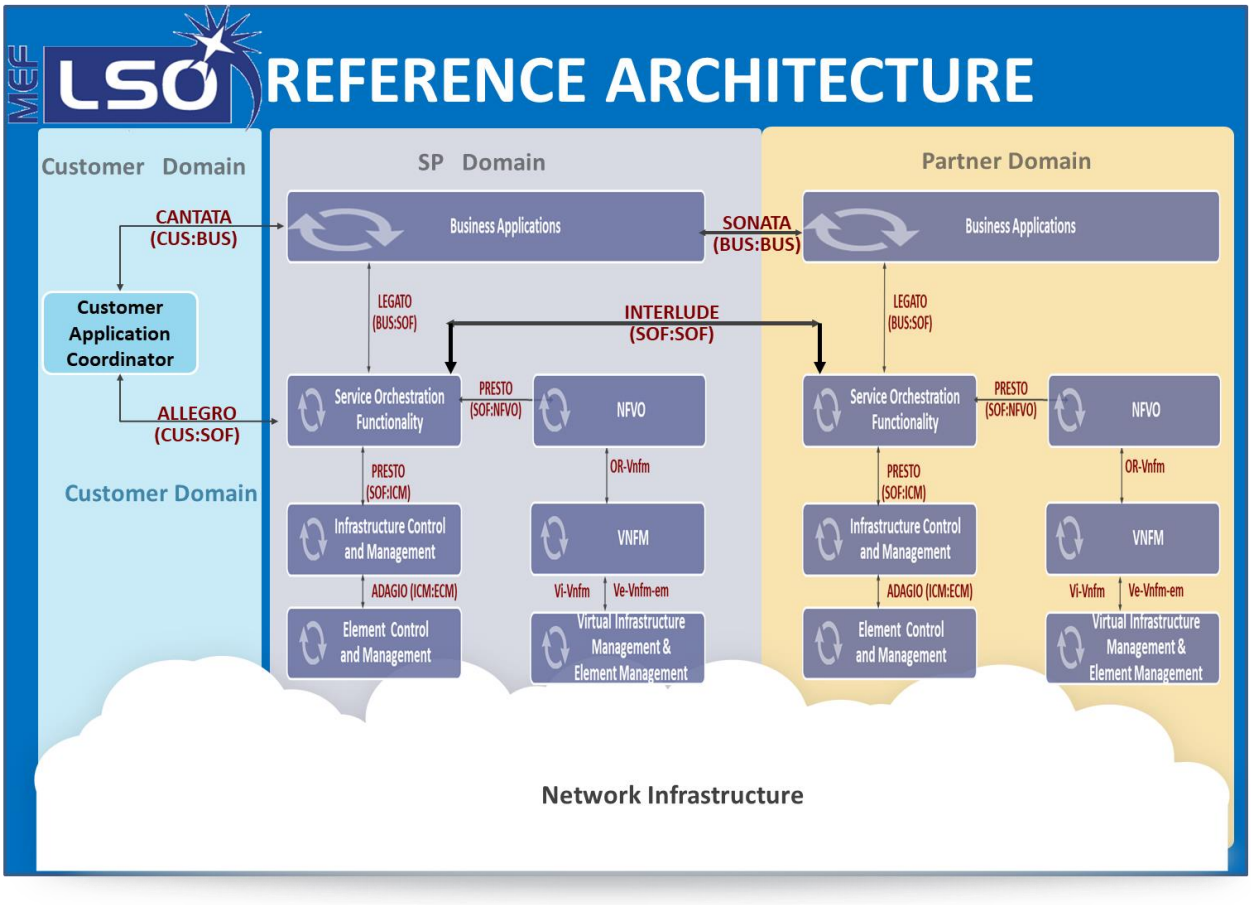
Figure 16 assumes automated end-to-end management of services riding over integrated resources of terrestrial and space infrastructure that make Network2030, via a federated OSS/BSS and Orchestrators. Each domain consists of management components to manage virtualized and non-virtualized resources of sub-domains (e.g. Infrastructure Control Management, Network Function Virtualization Orchestrator (NFVO), Virtual Network Function Manager (VNFM), etc.) and management components to manage nodes in each subdomain (e.g., Element Management System (EMS), Virtual Infrastructure Management, etc.).

In the federated OSS/BSS and Orchestrators, the interaction among OSS.BSS and Orchestrators take place over standards interfaces. **Figure 17** depicts the standards interfaces between user and a SP, management entities of a SP and a Partner within their own domains, and between OSS/BSS and Orchestrators of SP and Partner, where Partner is another Operator providing a segment of the end-to-end service provided by the SP to the user. These standards interfaces have been defined in [ARCH.4, ARCH.5]. In order to achieve true end-to-end automation, functionalities of these interfaces may need to be expanded. Furthermore, Application Programming Interfaces (APIs) of the standards interfaces among Operators, and between user and Operators are expected to play key roles in achieving the automation.

The architectures described in **Figures 16** and **17** are expected to support services from best effort SLOs such as Internet Access to services with very stringent SLOs such as self-driven cars. The management of services requiring very low delay and non-zero loss is expected to use Infrastructure Layer (e.g., SDN Controller, VNFM) and/or EMS Layer mostly while supporting the end-to-end coordination with the Orchestrator.



(a) LSO Architecture for a SP with both Virtualized and non-Virtualized Components



(b) LSO Architecture for a SP and its Partner Services, with both Virtualized and Non-Virtualized Components

Figure 17- Lifecycle Services Orchestration [ARCH.2, ARCH.3]

9.4 Conclusion

Section 9 provides a vision for data path and management requirements and architectures for automated and federated heterogeneous networks of Network2030 to support on-time and in-time services in addition to best effort services. The following sections are aimed to provide details how to achieve that.

10 Access Network and Edge

10.2 Introduction

Network2030 timelines may see very rapid innovation in the development of applications that are expected to require very stringent performance requirement (e.g., very low delay, jitter, bit error and packet loss; information security sensitivity, etc.) that may be difficult to meet with the current infrastructure. With enhancements in computing and memory technologies, it is possible to support these applications by devices located at the edge of Network2030 and/or customer premises.

These requirements are driven by the following trends:

- Densification of the edge through placing micro data centre capabilities;
- Innovation in future use cases e.g. Industrial automation, security and proactive monitoring, robotic surgery;
- Economics of network by optimizing backhaul and transport capacity through localization of content e.g., Augmented Reality/Virtual Reality (AR/VR) content, HD, Ultra HD Media content; and
- Economics of network through Multi-access Edge Computing (MEC) federation, collaboration and infrastructure sharing.

Existing Access and Edge network operation is already capable of localized traffic steering e.g. Local Internet Breakout or local content mixing in entertainment. Above mentioned trends further extend such concepts in network engineering with further innovation in technology and service domain.

Rapid increase in MEC deployment, localization of user plan and data plane processing near access network and ultra-dense access network will require innovative approach in designing Network2030. Future network needs to be service oriented, adaptive to change in operating conditions including environment, secure and capable of supporting multiple technologies at access and edge layer. Network2030 needs to be structured to provide easy integration with networks of multi-domains and collaboration among Operators and users.

Following are few elementary capabilities that Network2030 should support:

- Network2030 needs to support use cases emerging from service designs in area of in-time and on-time services. Therefore, access network and edge network need to be designed that they can provide guaranteed performance to support latency requirements associated with in-time and on-time services.
- Access network needs to operate in very uncertain environment (e.g., it is prone to disturbance in weather if access is wireless), it needs to balance very rapid and dynamic change in capacity utilization etc. It is also affected by natural and artificial noise that may affect appropriate service delivery. Therefore, access network needs a design that caters to complex operating scenarios so that it can provide desired QoS by adapting to changes in most efficient way.
- Access and Edge network need to support multi access technology and user plane data routing to the most optimal access technology based on service and user profile because user may have subscribed to multiple access technologies or user may be using telecom service for some essential or critical service.
- Access and Edge network is area that is prone to security and privacy breaches. Therefore, specific security and data privacy considerations associated with emerging use cases need to be supported in future network.

10.3 Access and Edge Components

Future Access and Edge network components are depicted in the figure below and described below.

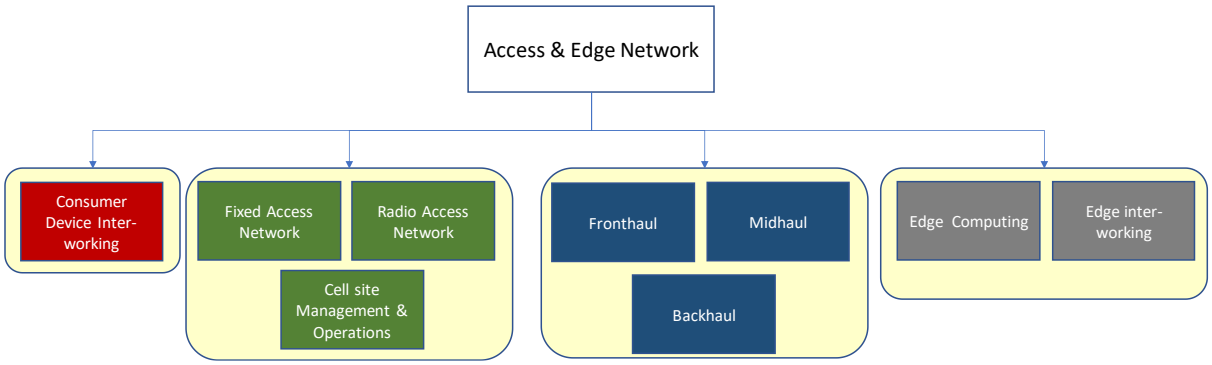


Figure 18- Access Components

- **Consumer Device Inter-working**- Network2030 consumer devices may be classified as
    - Human used devices,
    - Machine operated devices, and
    - Sensors.

These devices may require working intelligently in association with mobile or fixed-line network and may also require to work with peer to peer communication. The properties and aspect that assist in forming these devices part of access layer of network becomes important to be considered for future network innovation.

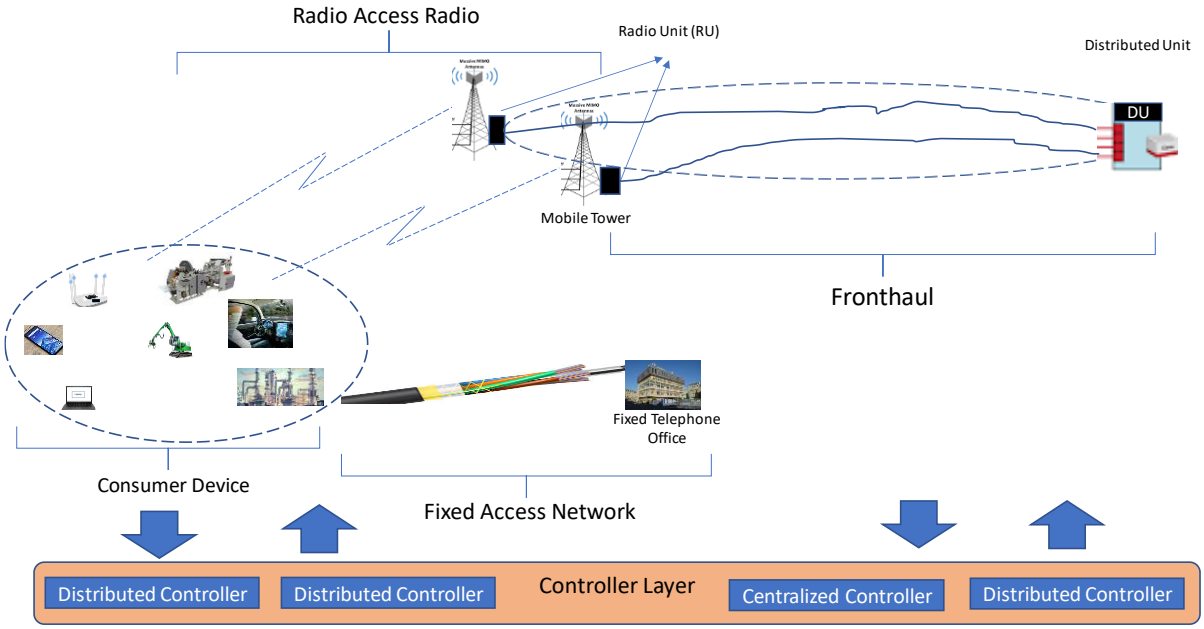


Figure 19- View of customer devices and front haul

Consumer devices can access connected world through fixed access or through radio network. Radio network may be based on any technology and first level of application of edge computing can happen just after termination of the radio traffic. Normally it is Radio unit of 5G or any similar unit of future technology. Further connection of the network traffic to next logical computing end is provided through network called as Fronthaul. Typically, it is up to DU (Distributed Unit) or any similar unit of future network. Enhanced Edge computing capabilities can be deployed at this point.

The use cases and communication service delivery platforms for quality sensitive services will require truly integrated last mile where actual service in the hands of consumer needs to be access network agnostic. Therefore, access and edge network solution need to provide similar performance irrespective of underlying technology. Edge computing at each compute node needs to provide comprehensive outcome that assures that customer is able to consume the service over diverse access network, therefore the above diagram includes both radio and fixed access scenarios.

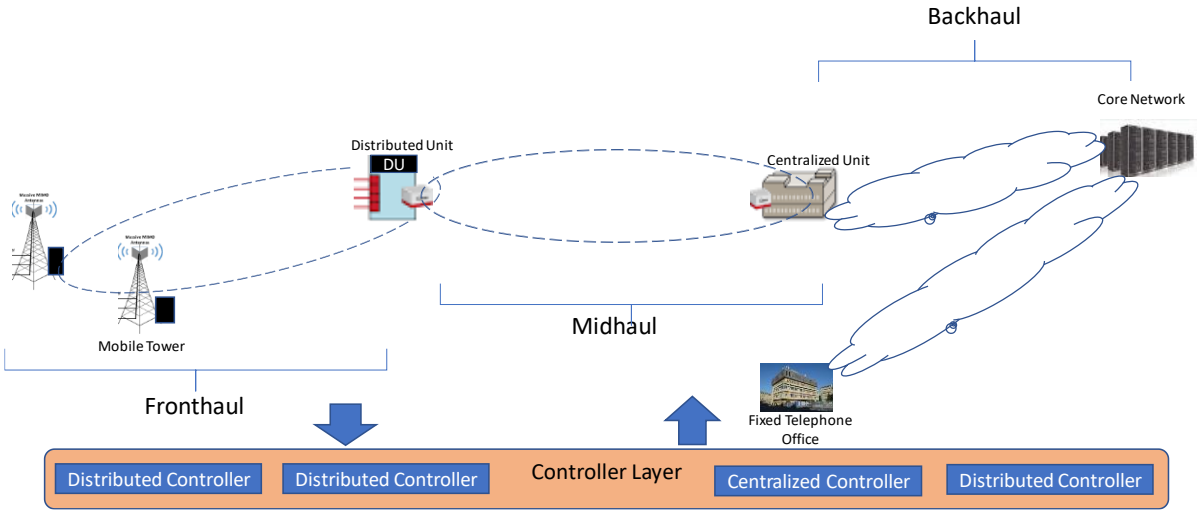


Figure 20- Fronthaul, Midhaul and Backhaul

Network elements of front haul are connected to core network through backhaul. To provide further computing and decision making, there may be arrangement of additional network traffic processing at the middle of backhaul through CU (Centralized Unit), therefore, making backhaul smaller. In such scenario, network between Distributed unit to centralized unit is termed as Midhaul whereas network segment between CU and core network is termed as Backhaul.

- **Radio Access Network**- Future network is expected to use heterogeneous wireless link layer to support multiple technologies & use cases. These aspects are considered under this section
- **Fixed Access Network**- Fixed access network enabling use cases for future society through fixed wireless or fixed copper/fiber are considered over here
- **Cell site management and operations**- Cell sites are integral part of network access layer. These may fall under edge design or next to edge design under various relevant use case designs. Considerations related to cell site design and applicable Management & operations functions is considered here.

- **Fronthaul**- Fronthaul may have multiple design options based on operating scenario, use-case and network properties. Fronthaul design requires due consideration for access network enablement in Future network
- **Backhaul**- Backhaul may be considered has hand off layer between access and transport/core network. Specific properties associated with access layer and Edge network of FG NETWORK2030 is studied in this section
- **Midhaul**- There may be need for deviation in design to put some network function & associated compute capability in the middle of Fronthaul and backhaul. Any such design aspect is provided due consideration over here
- **Edge Computing** - Various form of data and network layer analytics will be required to support use-cases requiring real-time decision making and management of data flow in intelligent fashion. This study may help in envisioning the requirements in the area of edge computing and analytics. Edge Computing may be at Mobile edge in the form of Mobile Edge Computing either at RAN or Fronthaul or mid-haul or backhaul or at the edge of enterprise/customer network. Edge computing nodes come with its own capabilities required to store processing data, compute or execute some algorithm and communication setup to interact with rest of the network
- **Edge Inter-working**- Edge inter-working among different stakeholders in future use-cases will become very important for successful delivery of designed services. Consideration of data aspect, integration aspect, security aspect and future requirement associated with coordinated inter-working is considered in this section. Edge inter-working may be with other edge computing nodes or with some industry vertical solution.
- **Controller Layer**- Controller layer hosts all controller applicable at Access and Edge layer to provide unified controller capability to underlying network.

  Controller can be network domain specific (e.g. SDN Controller, RAN Controller), network infrastructure specific (e.g. Slice Controller) or service specific (e.g. service quality controller).

10.4 Architecture

Figure 21 depicts a Network2030 edge architecture. At the right-hand side, the Internet access is provided through the peering with other domains, while localized service access is provided in customer networks. The service access relies on Point-of-Presence (POP)-based provisioning, e.g., through CDNs and other service platforms such as Google Cloud, AWS and others. The POP model will be complemented through the service rich multi-access, multi-technology and multi-ownership (in short *multi-X*) edge. This edge network will provide in-network edge clusters of compute resources, ultimately extended to the far edge devices, where said devices can become transient members of a specific service delivery relation. Note that within said model, particularly of multi-ownership, edge end as well as infrastructure devices may possibly be provided by private network owners, e.g., in industrial or entertainment use cases, even end users directly, e.g., in the form of home network based devices, in addition to one or more public network owner.

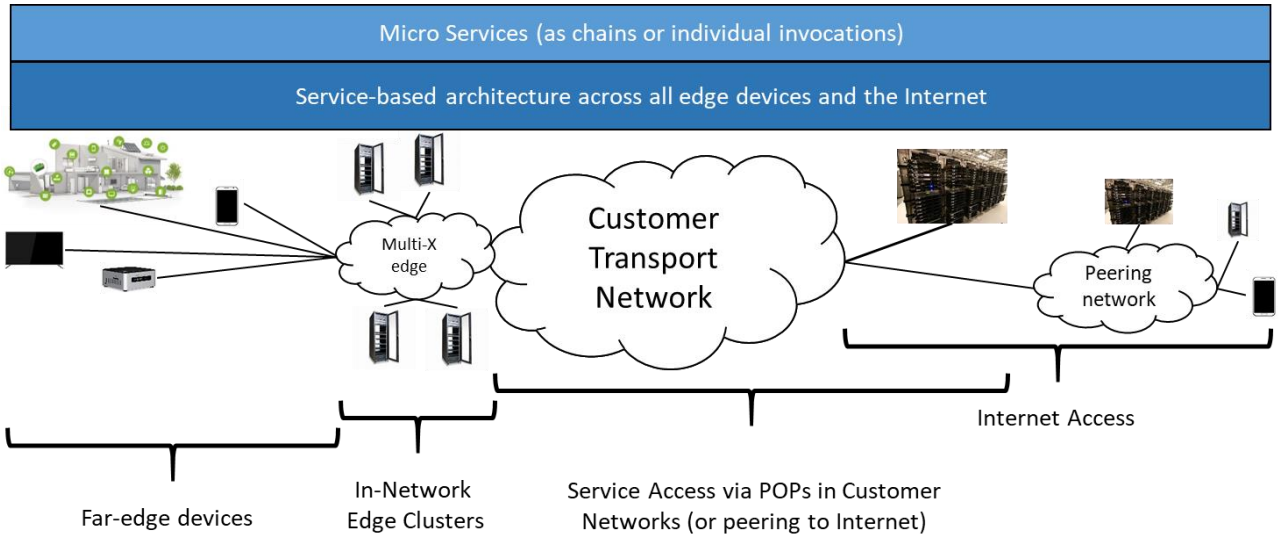


Figure 21- Edge Architecture

This transient nature of relationships constitutes a significant shift beyond the often long-term and static relations between network (operators) and end user (devices). Such transient relationships can be found, for example use cases such as Network and computing convergence (NCC) in [EDGE.4], but also occur in scenarios in which private network equipment, including end devices, is being utilized in the end-to-end provisioning of services to end users.

Figure 22 provides another view of Network2030 Access and Edge Network.

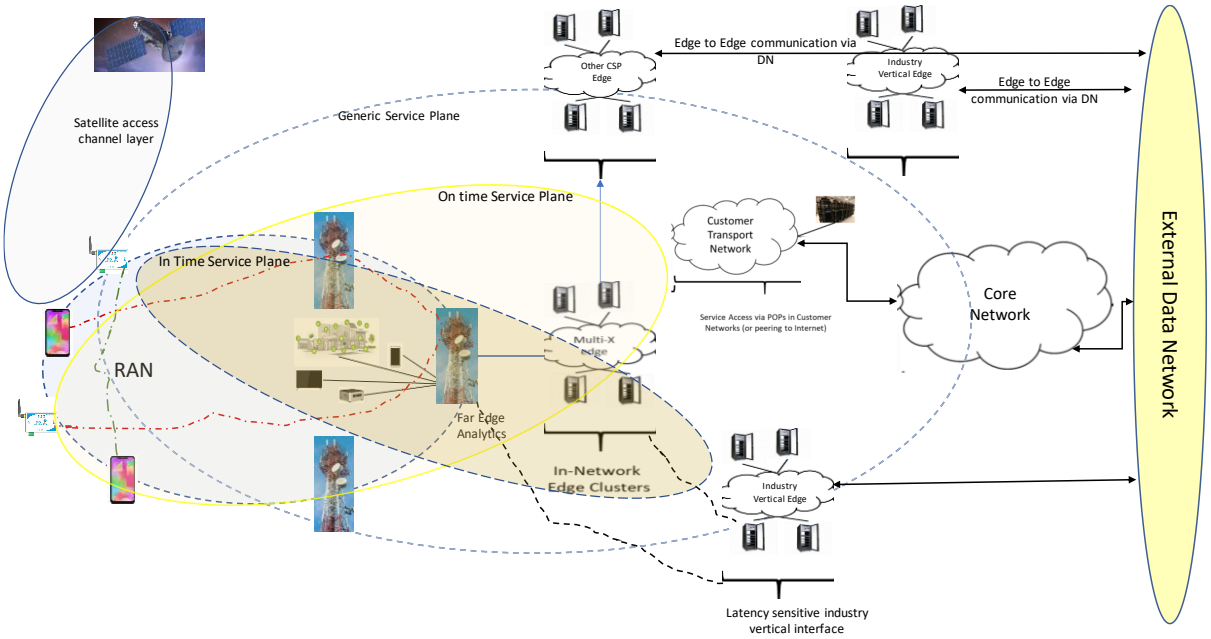


Figure 22- Future Network Access and Edge architecture

The access and edge network segments need to support the requirements outlined in the previous section. Hence, the architecture needs to be intelligently structured to support extreme operating conditions e.g. in-time and on-time service delivery, security and privacy, energy efficiency, dynamic service configuration, ubiquitous coverage, technology independence and quicker self-healing.

The architecture needs to adopt the following principles:

- Service oriented virtual network driven design to provide on-demand service plane for each service type e.g. dedicated plane for in-time service
- Multi-technology access network to provide unified features across heterogenous technology. Therefore, a service can be seamlessly ported from one device or network or technology to another device or network or technology.
- Distributed Edge computing close to Radio nodes for lower latency and rapid decision making
- Controllers to provide service, network and infrastructure management in distributed & centralized format so that localized Configuration, Management and Operation instructions can be implemented in real time while centralized decision making may happen at end to end network controller agent layer.

The architecture is divided into following parts:

- Device Centric Network- Device centric network provides device to device direct link for local communication e.g. device to device file transfer. Multiple devices can come together to form a specific purpose-based network to perform some use case. For example, local community discussions during lockdown. The setup and management can remain at macro-cell level or can be handed over to micro cell whereas data flow is directly from device to device.
- Radio Access Network- It is similar to prevailing radio units of mobile/wireless network:
- Macro Cell-Macro cells are for wide area coverage ranging in few miles;
- Micro Cell- Micro cells are for very short distance and can be further segmented into personal cell, femto cell, pico cell or any other form;
- Contextual/on-demand cell- Service provider may provision a cell for some contextual service that may be on demand. For example a virtual cell provisioning to support government administrative activity in high security service context during lockdown; and
- Satellite inter-working- Its details are described in Section 11.
- Access Radio Termination- Access radio termination that happens at Radio unit and provides a backhaul link becomes a major point of interface in access network. Since some compute capabilities in form of remote edge computing is established near radio unit therefore these termination points provide a demarcation area for traffic related decision making.
- Front-haul, Mid-haul & Back-haul (X-haul)- Traditional backhaul is divided into these three segments. Idea is to provide different compute and decision making capabilities at different points in backhaul network. Any edge computing in front haul will have less latency but will be more sensitive to storage and complexity of algorithm whereas any edge computing capability in backhaul may end up adding more latency but help in more centralized operation and hence storage and algorithm complexity can be built up. Mid-haul may be considered as a trade-off between front haul and back haul.
- X-Haul termination- X-haul termination refers to termination points for front haul or mid haul or back haul. It is used to create demarcation points and specify network segment as front haul, mid haul or backhaul.
- Edge Computing and Analytics- Edge computing and analytics is very critical aspect of future network because it provides localized data management, localized decision making, localized traffic offloading and therefore reduces latency as well as dependency on core network.
- Far Edge Computing and Analytics (Near Radio Unit)- This is capability hosted at remotest possible location.

- Concentric Decision Points and Analytics (Near Distribution Unit and Centralized Unit)- Edge computing at DU and CU helps in rendering local traffic off-loading and associated decision making.
- Edge to Core inter-working- Edge network needs to work in collaboration with core network. Though edge networks are provided with compute and storage capabilities, but these need to interact with core network in structural form so that end to end service delivery is not adversely impacted. For example avoidance of unlawful activities at access network.
- Edge to Edge inter-working- Edge network may need to interact with other edge network in close proximity to support use cases that are independent of core network. For example inter-community communication in close proximity or gaming tournament in local societies
- Edge to Industry vertical solution inter-working- Edge network of SP may require communicating directly with industry vertical solution in some scenarios e.g. local health center providing health services through automated local health center interface.

The architecture is visualized as service plane-based design where each plane is structured to cater to specific service parameters. Services may be allowed to navigate from plane to plane if there is change in service configuration or associated functional capability e.g. an in-time service may be moved from in-time service plane of low latency to on-time service plane of fixed latency.

10.5 Edge Computing and Analytics

Edge computing is extremely important for future network to realize many essential future use cases that are highly dependent upon low latency and jitter, and security and other quality parameters. ETSI listed following high-level concepts in its white paper [EDGE.1] that are essential in providing high performance Multi-access Edge Computing (MEC) services with an unparalleled quality of experience.

- Concurrent access to local and central Data Networks (DN) in a single PDU session
- Selection of the User Plane Function for a PDU session close to the UE's point of attachment
- Selection/establishment of a new UPF based on UE mobility and connectivity related events received from the SMF, see the "UE and application mobility" section
- Network Capability Exposure to allow MEC (AF) to request information about UE(s) or request actions towards UE(s), see the "Capabilities exposure" section.
- Possibility for MEC (AF) to influence traffic steering for a single UE or a group of UEs, see the" Traffic steering" section.
- Support for LI and Charging for MEC in the edge cloud, see the "Regulatory requirements" and "Charging" sections.
- Indication about LADN (Local Access Data Network) availability for UEs for specific and local MEC services.

One of the key aspects for future network will be to inter-work with edge network of non- mobile entities i.e. enterprise edge, industry vertical edge, ad-hoc network edge in mobile world or edge of fixed network. It is essential so that decision can be made at the edge of the interacting network segment and response can be provided to reduce latency and enhance network capacity utilization.

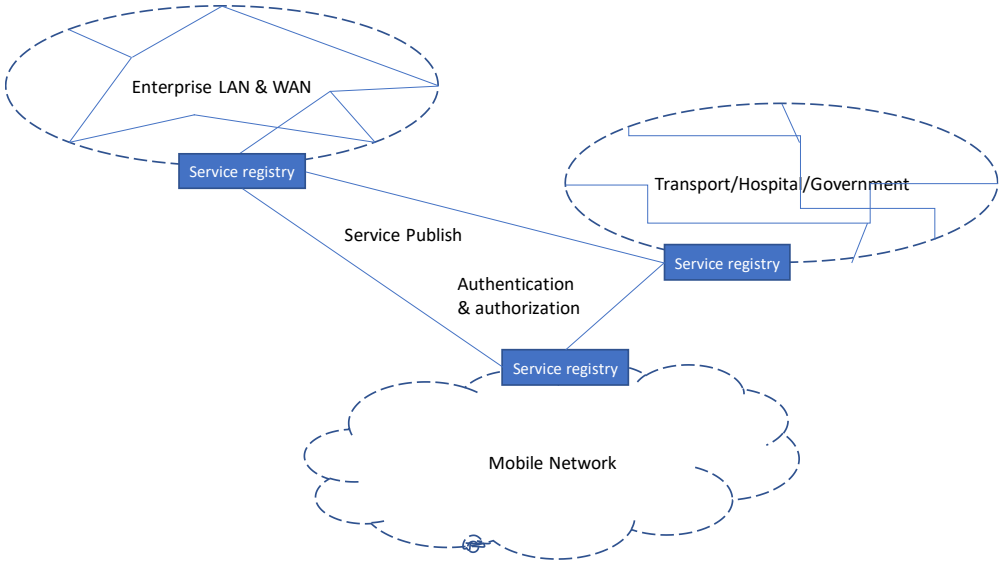


Figure 23- Edge Interworking

In MEC the services produced by the MEC applications are registered in the service registry of the MEC platform. Similar registries need to form an hierarchical interaction pattern across discrete network so that services can be exposed, subscribed & published, consumed, managed, rated & charged independently outside the network of a particular entity e.g. mobile service provider.

Edge of the network needs to have localized intelligence in deciding if received traffic has any relevance in further progression of the message or it can be terminated or if some extract of the data needs to flow further down. It is necessary to enhance the value of the capacity i.e. not merely acting as data flow pipe but working as intelligence flow pipes.

Another aspect of Edge computing that may help in addressing some aspect of latency and jitter sensitive applications may be moving away from authenticate & authorize as sequential activity to a parallel procedure where enabling service delivery while authentication and authorization happens through graded risk & AI&ML enabled algorithm.

ETSI foresees MEC as provider of a new ecosystem and value chain. Operators can open their Radio Access Network (RAN) edge to authorized third-parties, allowing them to flexibly and rapidly deploy innovative applications and services towards mobile subscribers, enterprises and vertical segments.

To facilitate MEC application design, MEC communications can be divided in phases:

- Phase 1 – MEC application packaging and on-boarding
- Phase 2 – MEC application instantiation
- Phase 3 – communication between client-side app and MEC app
- Phase 4 – usage of the MEC platform and services

ETSI has published ready to use APIs as listed below [EDGE.1]:

- Mobile Edge Platform Application Enablement API
- Radio Network Information API
- Location API
- UE Identity API

- Bandwidth Management API
- UE Application Interface API
- Fixed Access Information API

10.6 MEC and Access Network

MEC forms the basis of architecture for most of the use-cases or functional requirements identified in Network2030. However, actual need of MEC functionality may vary from use-case to use-case basis. MEC may find relevance starting from location near antenna to location near core. Therefore, exposure of MEC capability depends upon the location of MEC functionality along with the use-case that is addresses.

In a scenario where MEC may be allowed to initiate data plane activity through Application of Data Network to reduce latency immediately after getting service request but without waiting for authorization process to complete at control plane may also trigger need of control plane ML and AI function close to RAN so that probability and risk associated with individual service requests can be determined and applied in decision making:

- As soon as latency sensitive service initiated, MEC at data plane initiates fulfillment through data plane network functions. It is done post risk assessment that probability of failure in AAA is very low.
- Parallel authentication and authorization request is initiated towards control pane.
- Service data is processed, and data plane session is established up-to MEC layer.
- Service authorization is received at control plane
- Service is fulfilled.

Since control plane latency is higher as compared to data plane, the combined latency is reduced as critical services or recovery process in industrial automation may be delivered more accurately.

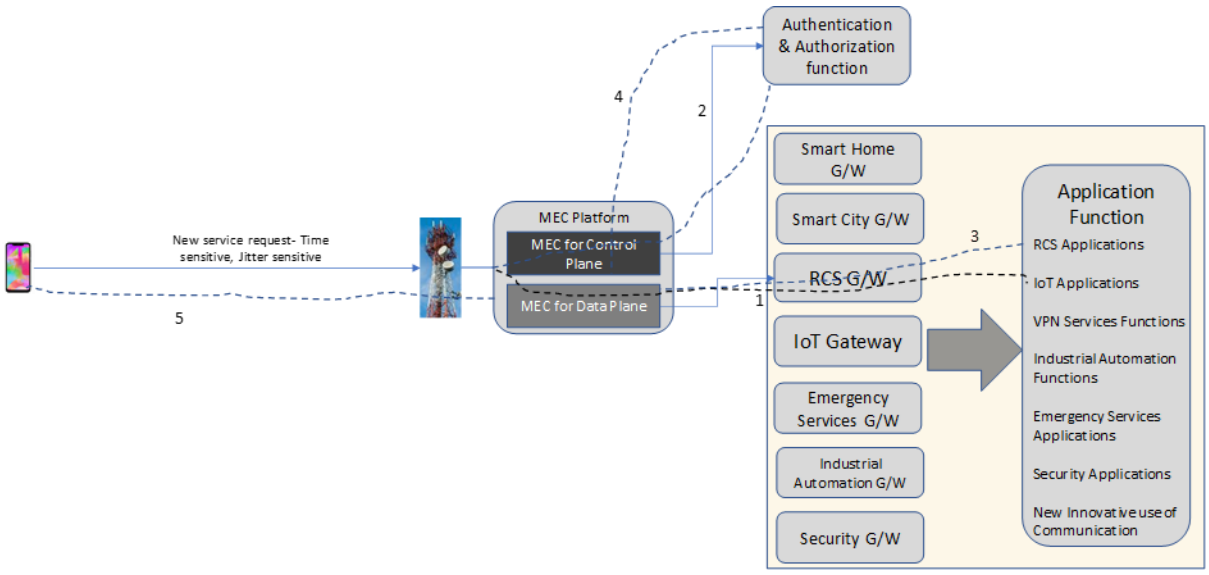


Figure 24- MEC and Access Network

10.7 Protocols and Interfaces

As we indicated in the previous sections, very low delay, jitter and loss for some of edge applications are important. In order to accommodate these tight performance requirements and optimize edge resources, a simplified addressing for the edge networking is needed. Name-based routing is an approach suggested here:

- **Services** are realized, for instance through known Interpret protocols, as residing directly on top of a name-based layer through **named service transaction** (NST)
    - **Names** are constructed as service identifiers linked to the specific protocol being realized on top of the named-based substrate
- Services can exist on several **service hosts**, realizing **service instances** of said service
    - Services can be established on-demand and quickly by virtue of virtualization and orchestration platforms
- Legacy devices/services are integrated through **proxy devices** at the network edge
- The name-based substrate operates on top of a **transport substrate**
    - Said transport substrate may utilize **path-based forwarding** of packets
    - Paths are constructed utilizing a **registration/path calculation** protocol
    - Path information is cached and **reactively maintained/updated** for resilience and adaptability to changing service instance availability

This approach that impacts the UNI and ENNI in Section 3 that are depicted in figures below.

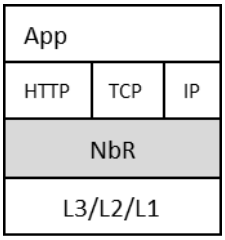


Figure 25- - Application UNI for Edge-Native Devices

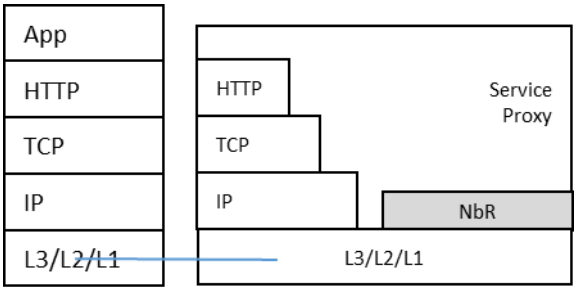


Figure 26- Application UNI for Legacy Devices

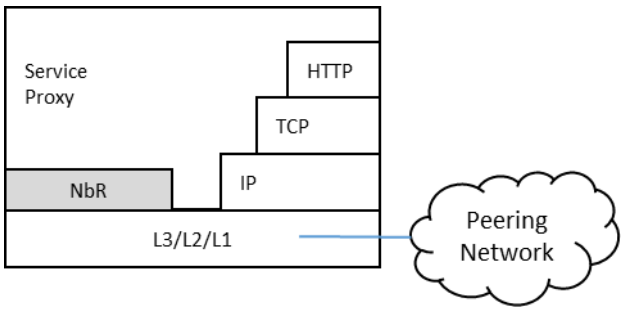


Figure 27- Edge Network to Peering Network ENNI

End-to-end packet flow based on name-based routing is depicted in Figure 30.

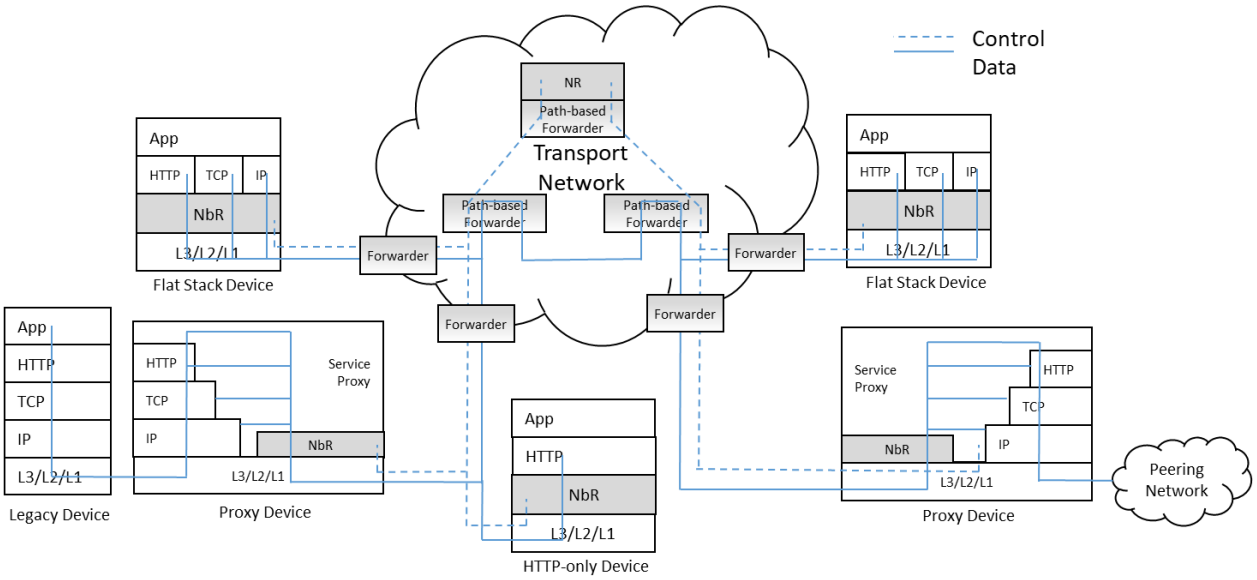


Figure 28- Protocol-Level Architecture of the Edge

10.8 Messaging Services

Messaging services are among the key edge services that need to be supported on future access and edge network. Messaging may be classified as

- One to One,
- Group Messaging,
- Multicast messaging, and
- Broadcast Messaging.

Future messaging involves multi-facet innovation making it feature rich and providing platform for person to person, machine to person or machine to machine messaging that can have features like:

- In flight message construct change (e.g. text to audio or video to text);
- Adaptive codecs and mode of delivery based on consumer properties, network conditions or other operating scenarios;
- Preventive fraud, fake messaging and securing personal data;
- Responsive to civil establishment and legal framework; and
- Multi-mode lawful interception.

Group messaging is a very common and popular social media service that can be deployed to add value to many applications. In current Internet, group-messaging is an app-server centric solution, i.e., every message incurs an extra-hop as it goes through a message server first and then relayed to the clients. Whereas the group-messaging has evolved in as an active real-time (not passive like email) mobility-centric (not pinned to a single device) utility which is critical to both personal and business

communications. Some issues with current server-based model which is essentially a unicast service delivery.

- In order to scale group-based communications the application servers require scaling up and down.
- The servers may or may not be location-aware. This some connections/parties get sub-optimal message deliveries. It adds additional hop to communication.
- Ordering and timing of messages may get skewed which maybe necessary for use of group messaging in mission critical situations. This could happen due to non-deterministic path to/from server to group-members.
- Possibility of server being a single point of congestion (due to server load), failures (server outage) and security-threat (compromised server may add un-welcome listener as invisible).

Network2030 architecture needs to support of group communications as a basic network service by supporting identification replication points and opportunities for dynamic multicast forwarding in the deep edge network.

Any solution needs to address issues of optimal replication, low-latency, dynamic membership, mobility and security.

10.8.1 Multi-User Group Messaging

Group messaging is a very common and popular social media service that can be deployed to add value to many applications. In current Internet, group-messaging is an app-server centric solution (i.e., every message incurs an extra-hop as it goes through a message server first and then relayed to the clients). Whereas the group-messaging has evolved in as an active real-time (not passive like email) mobility-centric (not pinned to a single device) utility which is critical to both personal and business communications. Some issues with current server-based model which is essentially a unicast service delivery.

- In order to scale group-based communications the application servers require scaling up and down.
- The servers may or may not be location-aware. This some connections/parties get sub-optimal message deliveries. It adds additional hop to communication.
- Ordering and timing of messages may get skewed which maybe necessary for use of group messaging in mission critical situations. This could happen due to non-deterministic path to/from server to group-members.
- Possibility of server being a single point of congestion (due to server load), failures (server outage) and security-threat (compromised server may add un-welcome listener as invisible).

Network2030 architecture needs to cater to support of group communications as a basic network service by supporting identification replication points and opportunities for dynamic multicast forwarding in the deep edge network.

Any solution needs to address issues of optimal replication, low-latency, dynamic membership, mobility and security.

10.8.2 Opportunistic Multicast

Most of the current Internet traffic is due to unicast delivery of relatively immutable content such as video or software to very large client groups. This has resulted in large amount of redundancy in network traffic, as well as creating capacity bottlenecks both in the core network as well as the server infrastructure serving

the content. Technologies such as content delivery networks (CDNs) help to spread out the network load, but are complex to manage, have inherent limits in terms of how rapidly they can react to changing network and server conditions, and cannot fundamentally reduce the network overhead arising from redundant unicast streams.

In contrast, opportunistic multicast delivery as a basic service is proposed to automatically deliver responses to quasi-concurrent requests in a single lightweight multicast transmission over L2. Unlike traditional IP multicast, this approach has no additional setup time overhead and it does not require per-flow state in the network. The time period (which we call the catchment interval) over which this process takes place can be flexibly configured on a per-service basis, further improving the opportunity for multicast delivery. For latency-sensitive services such as video chunk delivery short timescales are appropriate (100ms – 1 second for example), whereas for delivering software updates, carrying out DB or cloud service synchronization, and other relatively delay-tolerant service much longer timescales can be used. The gains from multicast delivery can be especially dramatic for highly popular content at peak request times (new episodes of a popular series becoming available for example). As an optimization (that can again be enabled on per-service basis) we can combine opportunistic multicast delivery with request suppression where the origin server does not even receive the redundant requests that would be replied within a time multicast transmission, thereby reducing the server load and costs for content delivery even further.

Any deep-edge service architecture needs to provide means to opportunistic multicast delivery by allowing for efficient multicast transmission at the level of the transport network in order to reduce traffic load.

Most of the current Internet traffic is due to unicast delivery of relatively immutable content such as video or software to very large client groups. This has resulted in large amount of redundancy in network traffic, as well as creating capacity bottlenecks both in the core network as well as the server infrastructure serving the content. Technologies such as content delivery networks (CDNs) help to spread out the network load, but are complex to manage, have inherent limits in terms of how rapidly they can react to changing network and server conditions, and cannot fundamentally reduce the network overhead arising from redundant unicast streams.

In contrast, opportunistic multicast delivery as a basic service is proposed to automatically deliver responses to quasi-concurrent requests in a single lightweight multicast transmission over L2. Unlike traditional IP multicast, this approach has no additional setup time overhead and it does not require per-flow state in the network. The time period (which we call the catchment interval) over which this process takes place can be flexibly configured on a per-service basis, further improving the opportunity for multicast delivery. For latency-sensitive services such as video chunk delivery short timescales are appropriate (100ms – 1 second for example), whereas for delivering software updates, carrying out DB or cloud service synchronization, and other relatively delay-tolerant service much longer timescales can be used. The gains from multicast delivery can be especially dramatic for highly popular content at peak request times (new episodes of a popular series becoming available for example). As an optimization (that can again be enabled on per-service basis) we can combine opportunistic multicast delivery with request suppression where the origin server does not even receive the redundant requests that would be replied within a time multicast transmission, thereby reducing the server load and costs for content delivery even further.

10.9 Resource Fairness

Recent interest in novel transport protocols such as QUIC has shown that the traditional end-to-end resource management model the Internet is based on is often suboptimal for modern services, with rapidly

changing routing patterns between several virtual service endpoints rendering classical TCP congestion control inefficient. Opportunistic multicast decouples the resource management of the access link (which will be handled by whichever protocol the client uses to access the involved service, typically TCP or QUIC) from resource management of the transport network. This creates first of all the opportunity to support fairness between different resource management mechanisms (with UDP and TCP being the extreme classical example), and also to optimize the network more aggressively than enabled by traditional end-point centric solutions.

Any deep-edge service architecture needs to provide means for fair transport resource management at an end-to-end as well as edge-to-edge level.

10.10 Flow Setup

One of the key latency bottlenecks in the current Internet is caused by the high flow setup latency, especially when transport (or higher) layer security is involved. Furthermore, many applications still rely (for reliability reasons and to simplify development) on non-persistent connections that get rebuilt for every individual request for content items, even if served by the same origin server. In contrast, our proposal enables (but does not require) splitting of the connection at the network ingress point. Since this is usually very close latency-wise to the end user, optimizing the residual latency in the core translates to substantial latency reduction at the edge, even if the client-to-edge connection establishment is not modified. Such approaches have been successfully used in the wireless community to deal with extreme latencies (as found in satellite communications for example), and our approach enables deploying them transparently at the network edge as well.

Any deep-edge service architecture needs to separate setup of long-term end-to-end as well as edge-to-edge flows from short-term end-to-end transactions to reduce setup latency of the latter.

10.11 Efficient Transport Network Integration

The proliferation of software-defined networking (SDN) but also new overlay transport concepts such as Bit Index Explicit Replication (BIER) [EDGE.5] is utilized by mobile and fixed customer network operators alike to transition towards a simplified infrastructure at the level of Layer 2 with abstractions such as Ethernet provided to higher layer services. Flow-based forwarding is the currently dominating form of forwarding operation with, e.g., OpenFlow based forwarding rules being used to realize forwarding decision in intermediary switches, coming with the well-documented limitations in terms of flow table growth. The approach of path-based forwarding for SDN utilizes link information instead, combined into a unique path information that can be used through simple binary operations in each switch to make forwarding decision, leading to a constant forwarding table size, as documented in [EDGE.6] and also used in the BIER-TE efforts [EDGE.7]. Those efforts show that efficient integration into the transport network is a crucial aspect in edge networks, particularly in combination with the opportunistic multicast requirement in Section 10.8.2.

Any deep-edge service architecture needs tos provide efficiently integrate with the (emerging as well as existing) transport network infrastructure for wireless, fixed but also mobile networks to not only reduce or limit total cost of ownership but also enable opportunistic multicast capabilities at no or limited additional costs.

10.12 Deterministic Networking

As the end-to-end latency and latency requirements for edge services are expected to be in the order of milliseconds, or even sub-millisecond in extreme cases, The low-latency services are to be provided through access to local edge computing and storage resources.

Depending on the specific application requirements, there should be a need to implement deterministic networking and/or time-sensitive networking (TSN) profiles.

This places requirements on the incorporation of specific queuing algorithms/disciplines, such as priority and frame pre-emption queuing, synchronized port gating, and persistent and semi-persistent scheduling super-imposed over random access or request/grant access procedures. In some cases, delay variation requirements may be met through the use of buffering, but in these cases it will often be the case that precise playout times for the user data will be required. There may be other requirements for precise time synchronization of network elements, for example, in accurate localization.

Thus, to meet such requirements, the deep-edge service architecture needs to be able to support the use of precision timing protocols, enabling time synchronization to nanosecond accuracy.

10.13 Ultra-Reliable communications

Some of edge services require guaranteeing packet delivery (99.9999%) over networks, which may be noise, interference or congestion limited. Examples for these applications are emergency services, requiring remote operation of equipment, with/without augmented reality, for industrial automation (Industry 4.0) requiring remote control/operation of equipment moving between machinery, and for vehicle-to-vehicle and vehicle-to-infrastructure communication for (semi-)autonomous driving.

For such mission-critical applications, enhanced forward error correction and coding schemes should be applied, where these may need to take into account short control message lengths. This may require some joint L1/L2 mechanisms.

The reliability should be augmented by mechanisms such as packet/frame replication, forwarding over diverse paths and duplicate elimination. In many cases, the requirements for ultra-reliable communications will intersect with those for low latency. Thus, new joint encoding schemes, and frame replication and duplicate elimination mechanisms MUST be latency sensitive.

10.14 End User Equipment Interaction with MEC

MEC federation and collaboration provides an opportunity to increase performance of user equipment by shifting most of the high processing, memory hungry and bulky applications at the edge of the network. Traditionally mobile applications are installed at user device which require frequent updates. These need native processing capabilities, memory and energy of the device. With the help of edge platforms, such applications can be hosted outside device and accessed by standardized APIs which are independent to native OS of the device. Only Location of the edge hosting depends upon the need of latency, accessibility, data processing and criticality of the applications i.e. if application is very sensitive to latency then it needs to be hosted near radio edge but if its not so sensitive then it can be pushed towards backhaul. This will not only reduce memory and energy requirements of the user equipment or device but also reduce the cost of the user equipment. It will also reduce dependency upon physical device i.e. porting of device will become very easy.

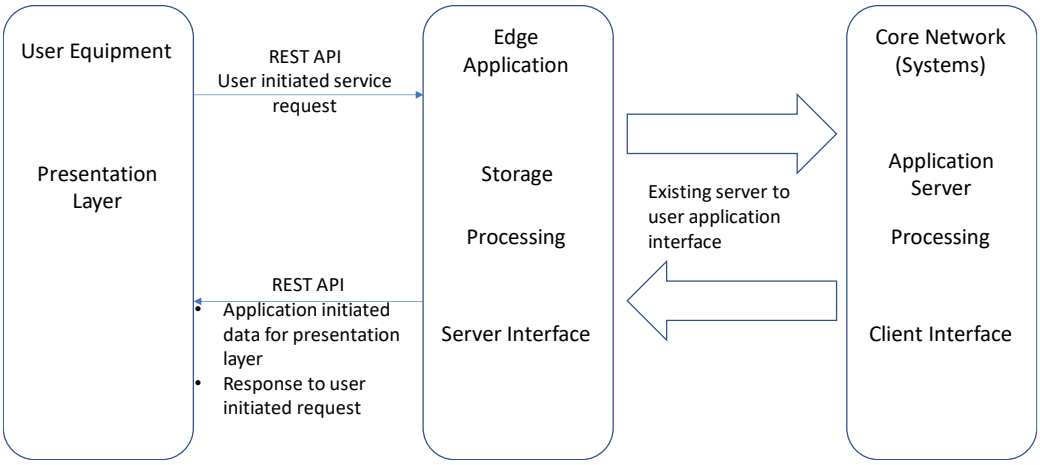


Figure 29- Three tier distributed application functions view

The above advantage of the MEC federation & collaboration poses new challenges that need to be addressed. These are followings

i. Support for situations when user equipment moves out of the edge of the network or moves into different edge i.e. need of support for roaming across edge networks.
ii. API security at application layer to make sure that service calls are from certified users
iii. Hardware and software upgrades at Edge

First point above is associated with mobility and communication industry has been very innovative in addressing this. In present context, it may be more challenging because here data requirements, application knowledge and accessibility all are involved at the edge of the network. It is not possible to overload edge of the network with features that can reduce efficiency of the edge itself.
Following approach can be followed

a- Applications not susceptible to high latency- The applications which are not very susceptible to latency may remain in native Edge and can be accessed in same way as any RCS feature is accessed in future network. There can be an additional identity i.e. Edge ID along with application ID that can be stored in databases like UDM to support roaming scenarios.

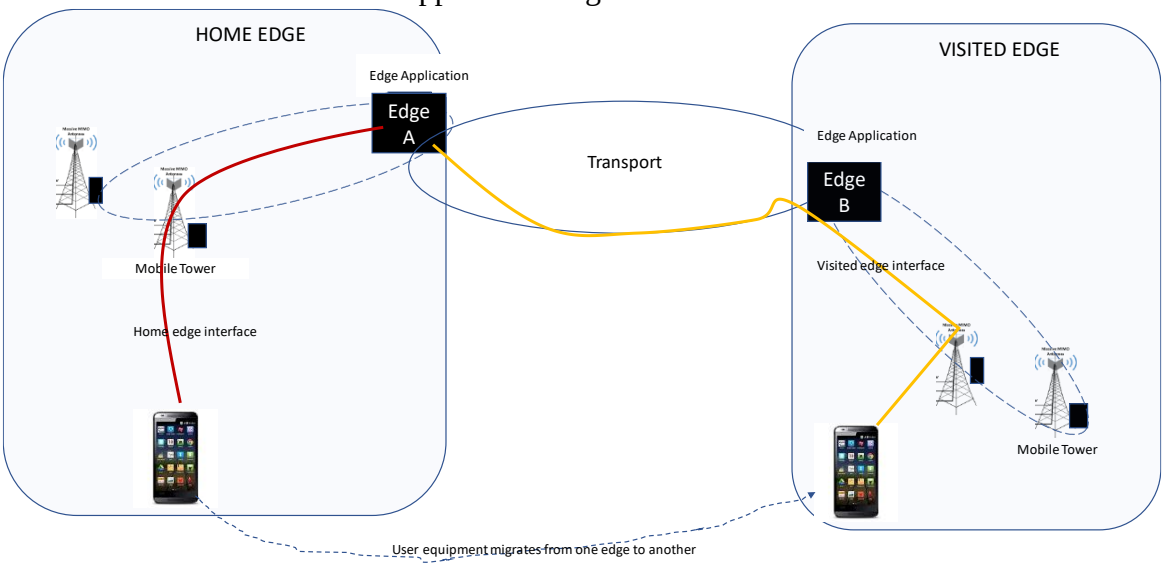


Figure 30- Roaming of user equipment in new Edge for non-critical applications

b- Applications susceptible to latency- The applications which are susceptible to latency need to move to new edge of the network where user equipment has moved. It is because latency involved in accessing the application cannot be increased or compromised. It is essentially important for in-time or on-time applications. Here roaming will have to supported along with Edge user application or edge service function porting.

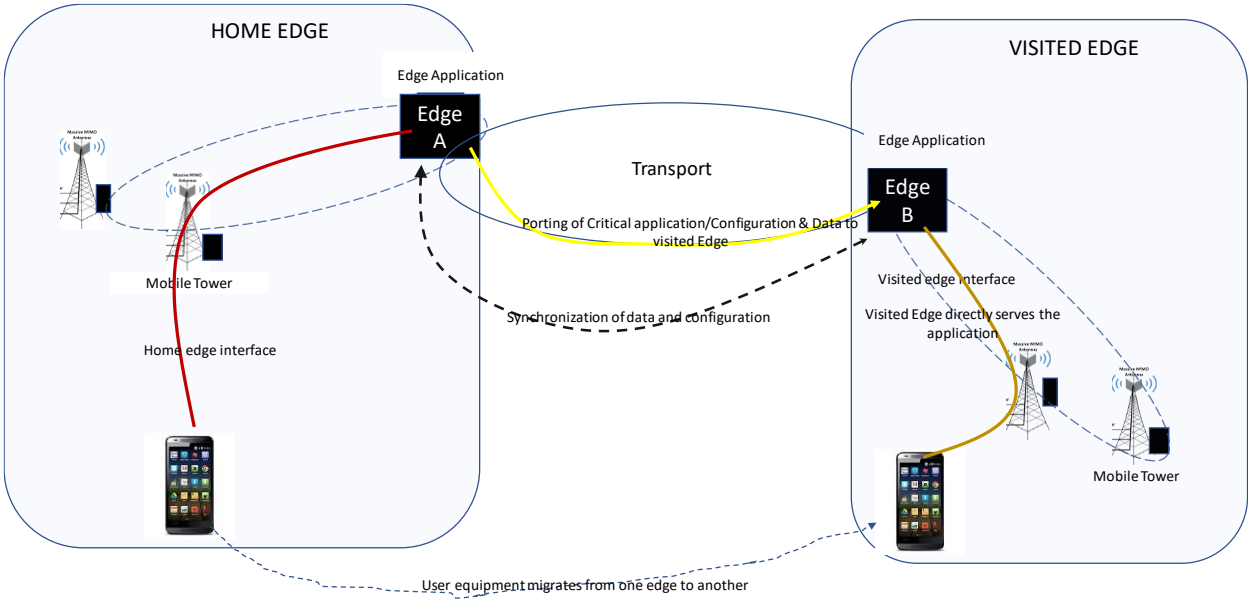


Figure 31- Roaming of user equipment in new Edge for critical applications

Following sequence diagram may provide a view on proposal of either application porting or porting of configuration and data associated to device in visitor network.

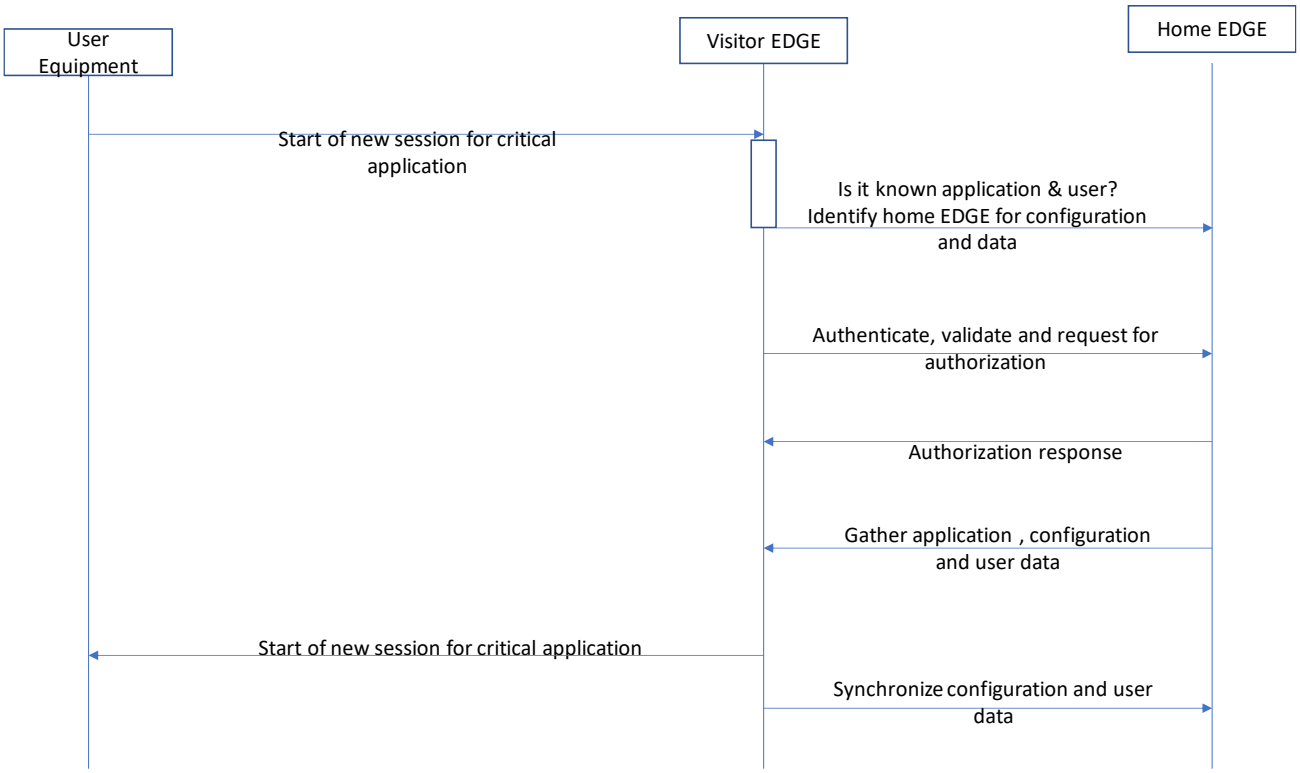


Figure 32- Key activities in new Edge for critical applications for roaming user

It is understood that there may be some critical and data sensitive critical applications that cannot be used when device is not in home EDGE. It is because some applications will have highly sensitive user data, may have some copyright problems in sharing to new EDGE (specially if E/AO is different) or may not be supported with minimum required quality parameters. Therefore such applications will not be available in visited EDGE but these are going to be very small in numbers and industry may evolve to fnd some way to address these challenges.

10.15 MEC Federation and Collaboration

Network2030 is providing foundation to many innovative services. Growth in service innovation provider many opportunity and challenges to Service Providers (SPs). Opportunities come in form of providing better service than competitor, becoming more relevant to society and solve complex problems in human civilization through capabilities of the communication service. Challenges come in many forms and some of them are related to management of complex eco-system of service platforms, seamless integration with non-telecom capabilities, managing balance between cost and benefits and remain innovative from new service feature perspective.

One of the sharpest arrows in the quiver of SP and Edge/Access Operator (E/AO) is federating capability and becoming part of collaboration with shared risk and cost. SPs and Edge/Access Operators (E/AO) have been doing infrastructure sharing since long and infrastructure sharing provided sustainability to telecom industry through shared cost and risk.

Future of communication service is evolving around platforms and freedom from very heavy core network systems that historically provided a monolithic structure to SP and E/AO. SP and E/AO are pushing more capability towards edge of the network and MEC is proving exceptionally beneficial because most of the analytical functions can be logically hosted at MEC platform and service configuration can be routed through MEC based capability.

Therefore, adopting federation and collaboration at service platform, especially MEC layer capabilities may prove boon for SP and E/AO who are consistently chasing the high paced innovation in service domain. MEC federation and collaboration provides a unique proposition in multi-industry services e.g. Industry vertical solution or industrial automation.

There are, multiple ways through which Service Providers & Edge/Access Operators (E/AO) can take advantage of MEC federation and collaboration. GSMA has put forward “Operator Platform Concept” in its white paper published in January 2020 [EDGE.2].

10.15.1 GSMA Operator Platform Concept

Operator Platform is a set of functional modules that enables an operator to place the solutions or applications of enterprises in close proximity to their customers. SPs and E/AOs can monetize and exploit service capabilities such as edge cloud computing capabilities, IP communications or slicing in a scalable way and in a federated manner with other SPs and E/AOs.

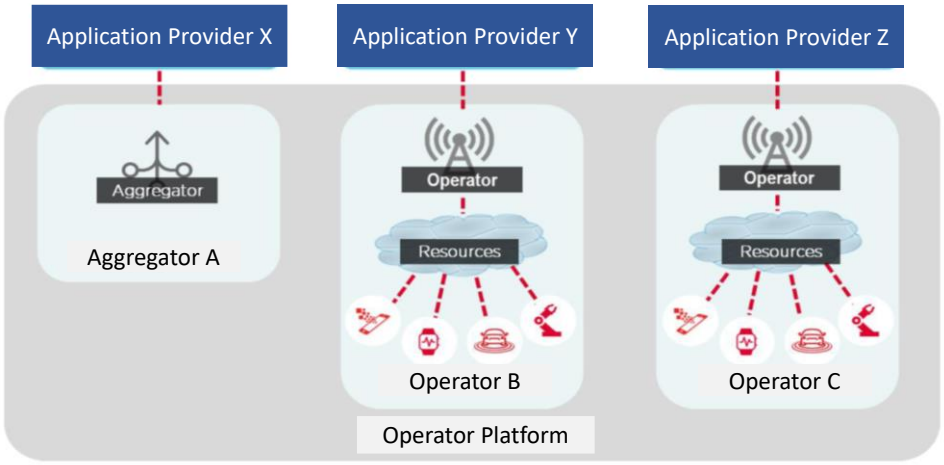


Figure 33- Operator Platform View [EDGE.2]

10.15.2 MEC Federation and Collaboration

The proposed concept of Operator Platform of GSMA can be further extended and converted into a completely open collaborative MEC platform where service capabilities are hosted into MEC platforms and offered as an independent service to any E/AO or enterprise. MEC capabilities can be extended from MEC to MEC integration of MEC capability providers that may be point to point communication or through wide area network cloud.

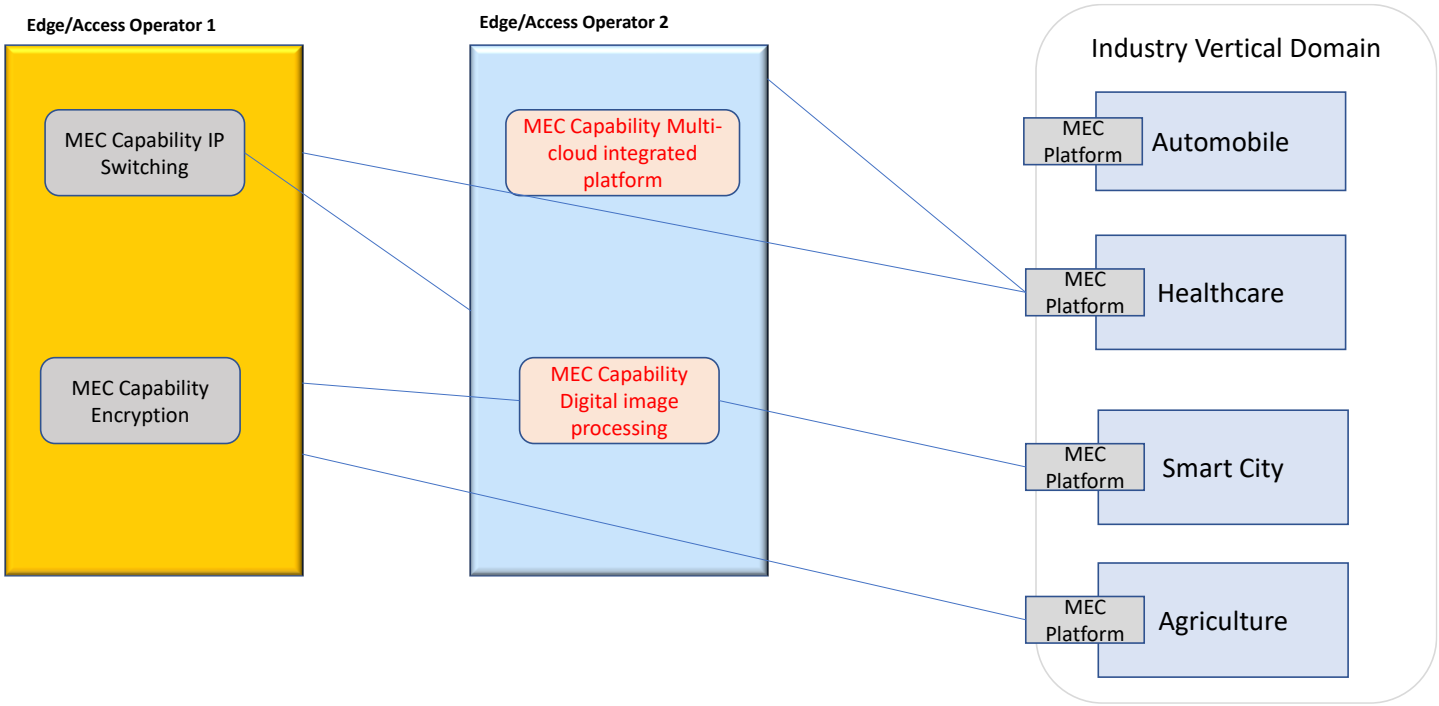


Figure 34- E/AO provided MEC platform and Collaboration

Service capability built and offered at a MEC platform of a E/AO or Industry vertical solution provider can be extended to any other Service Providers or E/AO or enterprise consumer. There can be pure play independent service capability providers that specialize and build service capability to offer them to any Service Provider or service consumer. GSMA identifies role of aggregators in its Operator Platform where an aggregator can create a composite service i.e. service involving multiple capabilities or aggregate services offered by multiple players. In broader terms aggregators can be further generalized in form of traders or brokers that collaborate with multiple service providers in multiple geolocations. These traders or brokers negotiate on commercial and service performance parameters to provide optimum offer to respective Service Provider or Edge/Access Service Provider or enterprise consumer. Here these are called as “MEC capability broker and Aggregator”. MEC capability broker and aggregator can create end to end service by joining MEC capabilities from various MEC capability providers in form of MEC capability chain and offer this chain as complete service to Service Provider or Edge/Access Service Provider or Enterprise Customer.

In this way, federated environment of MEC capabilities create an eco-system of additional business models, shared risk and optimized operations for E/AO.

Following Diagram provides an End to End view for MEC capability collaboration.

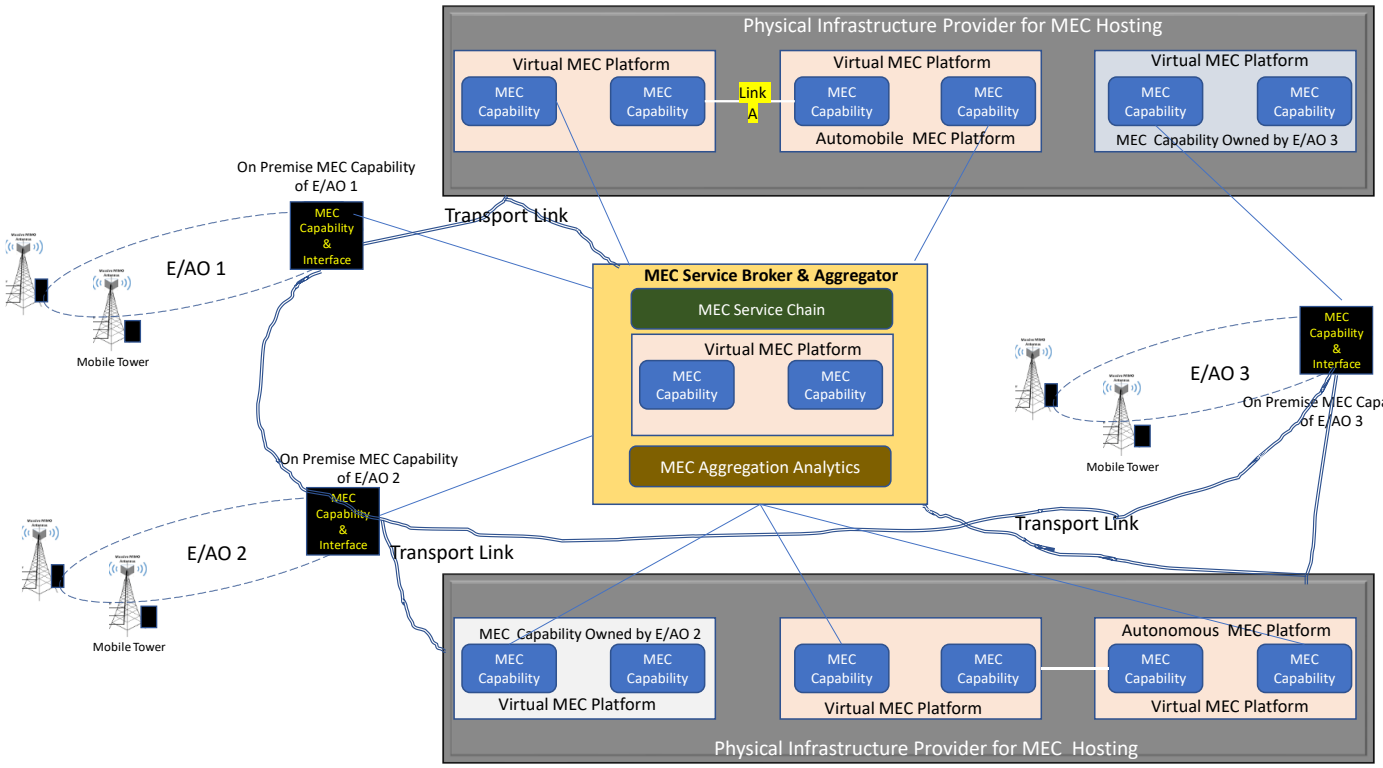


Figure 35- End to End view for MEC capability collaboration

The above diagram has following components and actors:

- E/AO- E/AOs are Access and Edge network operators that provide respective Edge/Access service by using network and system capabilities including MEC. E/AO can have their own MEC capability that they may host in their respective datacenter or they can host in external datacenter that can be provided by any independent MEC infrastructure provider or by MEC aggregator.
- Physical Infrastructure Provider- These are common infrastructure provider where any virtual system or platform can be hosted. These infrastructure providers can provider same physical infrastructure to multiple virtual platform/system owners in shared fashion.
- Virtual MEC Platform Providers- Virtual MEC platform providers provide virtual infrastructure and associated capabilities e.g. OS/Hosting Platform/Security etc to MEC capability provider. Individual virtual platform can host multiple MEC capabilities from same E/AO or MEC capability provider or from different E/AO or MEC capability provider. By providing shared cost mechanism such collaboration optimizes effective cost for each Service Providers and Edge/Access Service Providers (E/AO)
- MEC Capability Provider- Anyone with good MEC idea and built component of the idea may offer MEC capability to Service Providers and E/AO or Industry vertical solution providers .E/AO and Industry vertical solution providers can also host their own MEC capabilities and offer to other SPs, Industry vertical solution provider or any other enterprise customer. For example End to End encryption may be one service that can be hosted at MEC and can be offered to any Service Provider, enterprise or Industry player with equal importance.
- MEC Service Broker and Aggregator- MEC service brokers and aggregators play important role in negotiation and establishing complete service delivery by combining MEC capability provided by different providers. Service Providers and E/AO can have direct commercial and technical

service delivery relationship with other MEC capability providers or else they may do so through MEC service broker & aggregator. MEC service broker & aggregators become more relevant in value chain when each MEC capability provider provides only atomic MEC service that is not complete in itself for delivery of end customer service

- Transport Link providers- SP and E/AO can have their own respective transport and connectivity service between different MEC platforms or they may take it from other long-distance connectivity providers.

10.15.3 Business Benefits

Following are key business benefits in using MEC federation and Collaboration:

- E/AO can host its MEC capability on any shared platform to save cost
- E/AO need not to build any MEC capability for immediate need or temporary requirement
- E/AO can offer its MEC capability to other SP or enterprise to recover its cost quickly
- SP can prefer to partner with an Edge/Access Operator to support the capability
- MEC platforms can be used at optimal capacity by sharing spare capacity with others
- Enterprise customers or end users do not need to have multiple contracts in lack of capability at its service provider because service provider will have flexibility to bring in capability/application from other service providers

10.15.4 Business Value Chain

Following diagram provides a value chain view for proposed MEC federation and collaboration

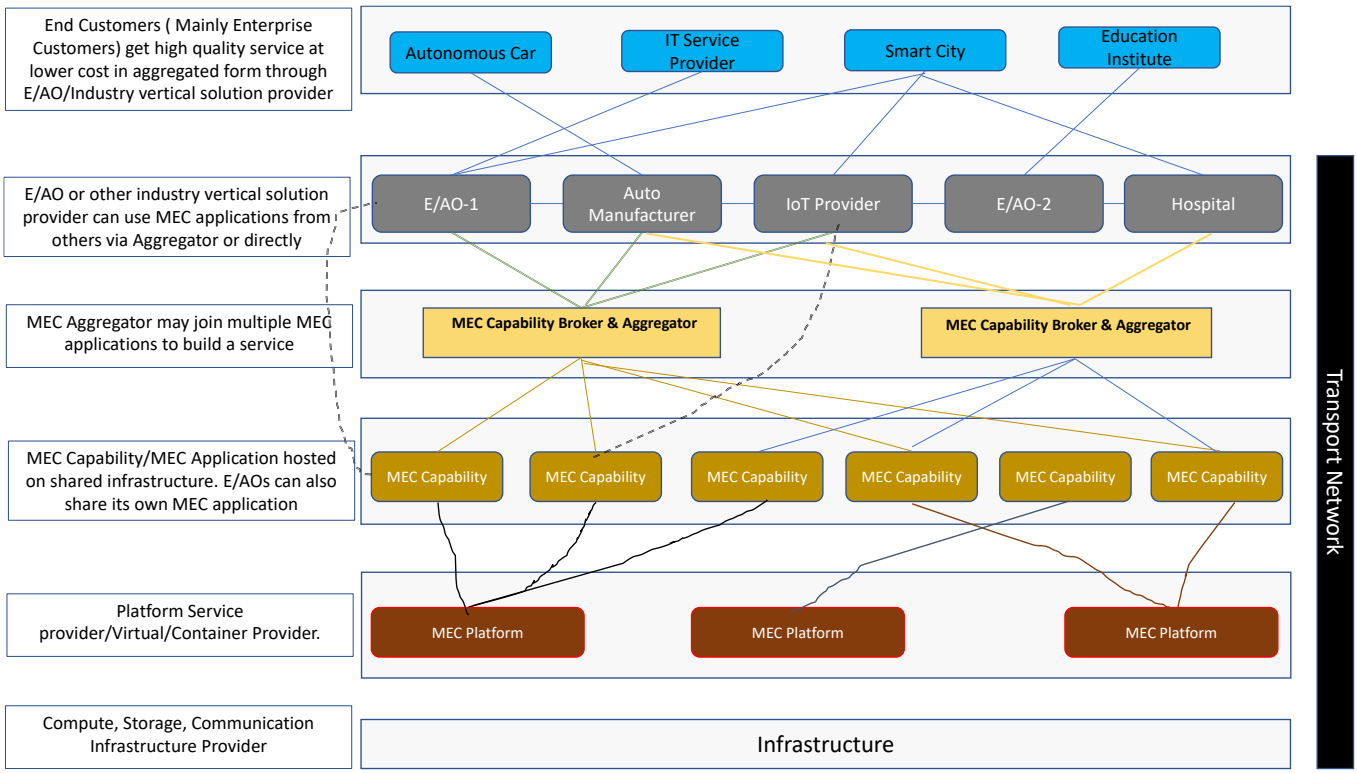


Figure 36- Shared eco-system

As described in the diagram above, federated model of deploying MEC capability by choosing strategic location and offering that as independent service to other service providers create a new eco-system of shared business models where business risk is reduced and profitability is increased.

10.15.5 Challenges and Remedies

The proposed methodology for MEC federation and collaboration has some intrinsic challenges but most of the challenges may be addressed and resolved. One of the major challenges is around contract agreements and performance tracking among roles in this value chain. This can be resolved by defining stringent KPIs and categorization of entities based on past performance.

A challenge arises around payment and settlement. Communication industry is having established practice of, multi-party settlement (e.g. roaming settlement, Settlements for transit links, etc.). This challenge can be addressed through established practice or by adopting more advanced multi-industry solution e.g. Blockchain.

Security and privacy are another challenge. This challenge is very important because different countries have different privacy and security legal framework and MEC capability provider may be providing service to any country in the world. This challenge can be addressed through existing practices of global operation in telecom industry while supplementing through localized rules via MEC Capability Broker and Aggregator.

10.16 Conclusion

Network2030 needs to support multiple access technologies and service scenarios therefore access and edge network needs to be inclusive of emerging services and innovation in applications. Network2030 access and edge network needs to support service porting from one technology to another so that irrespective of underlying network design users and devices can continue to consume services in all operating scenarios.

Network2030 design requires a lot of complex technology adoption, therefore access and edge components of the network should also support adequate federation and sharing. Critical services, Open APIs and sharing of compute network will have added need for new security and privacy solutions at access and edge layer.

11 Space Networking

Satellite-based networking, or say space network, can bring benefit especially in the long distance communication [1] and wider access coverage especially in rural areas. The space network has been considered as one of the important components of 2030 network. The future space network can not only work internally, but also cooperate with the existing network infrastructures and then become a space-terrestrial network, which intent to deploy a unified network protocol suite. This document aims to highlight specific scenarios and our envisaged technical challenges in the future integration of space networks with the current terrestrial Internet infrastructure in a seamless manner. Here we mainly focus on the Low Earth Orbit (LEO) satellite system which is able to provider low end-to-end latency as compared to its GEO (Geostationary Earth Orbit) counterpart. The common vision in this scenario is that multiple (up to thousands) LEO satellites can be interconnected to form a network infrastructure in the space which will be further integrated with the network infrastructures on the ground. On the other hand, the key challenge in this case is the frequent handover between the two networks caused by the constellation behaviors at the LEO satellite side. The rest of this document aim to describe in details different strategies for such network integration and also the specific technical issues that need to be addressed.

11.1 Key Components of Future Integrated Space-terrestrial Network

- **Satellite***:* Low Earth Orbit (LEO) satellite has lower physical orbit which potentially bring the short latency benefit. Medium Earth Orbit (MEO) and Geostationary Orbit (GEO) can provide more physical stability. The current satellite system mostly provides relay function however in the future the satellite system may build up a mesh-like network then provide routing and forwarding function. The LEO should be organized as routing system and work as router. The MEO and GEO may also play the role of router but work as complement and control function further.
- **Ground Station and Terminal:** Ground station and terminals are a type of physical terrestrial devices that act as gateway or interfaces between terrestrial and space networks through radio communications. At present, the networking mechanisms and protocols used in space networks are different from that in the traditional IP framework in the terrestrial infrastructures, and hence ground stations and terminals have been responsible for protocol translations and creation/maintenance of tunnels in order for data packets to traverse different network environments.
- *Controller (SDN architecture-based)*

The satellite network system may also employ hierarchical architecture. So some of the satellite not only play the role of router but also controller. Refer to SDN, the MEO and GEO may stand higher layer and control the low layer devices (LEO) which are expected to take the role of data forwarding in the data plane.

- *Mobile Edge Computing (MEC) server*

MEC has been a terminology mainly in the context of 5G where local computing and storage capabilities can be embedded at the mobile network edge in order to provide low latency data/computing services to locally attached end users. It can be envisaged that in future emerging space and terrestrial networks, LEO satellites can also become MEC servers in constellation in the space once equipped with computing and data storage capabilities.

11.2 Fundamental integration use cases and scenarios

In this section we describe two different use cases in integrating LEO satellite network with the terrestrial infrastructures. The first use case is to use networked LEO satellites to providing transit service as backbone infrastructure in the space, while the second use case is to use individual satellites taking the role

of access nodes. Within the first use case we further spilt into two different scenarios of using LEO satellite network as backbone. The decoupled scenario is based on the availability of peering links between LEO satellites in the space, in which case the routing infrastructure can be completely decoupled from its terrestrial counterpart. In comparison, in the couple scenario there is no peering link between neighboring LEO satellites, and hence each LEO satellite can be independently deemed as an "overlay" node on top of the terrestrial network infrastructure. The main reason for this situation is the current difficulty in establishing peering links between satellites due to the limitations on the antenna design. So without loss of generality we elaborate on specific features based on both scenarios.

11.3 Using LEO satellites as backbone network

11.3.1 Decoupled scenario

This is a more traditional view on the internetworking between LEO satellite network and the terrestrial infrastructure. Thanks to the availability of peering links between neighboring satellites, it is possible to deploy a completely different routing mechanisms among satellites which do not need to rely on terrestrial routing infrastructure. As shown in **Figure 37**, the default scenario here is that once user data packets have been injected into the space network, they will only need to return back to the ground when reaching the last-hop satellite which is closest to the final destination. The delivery of the packets is based on dedicated routing mechanisms in the space network which can be completely different from that on the terrestrial infrastructure.

.

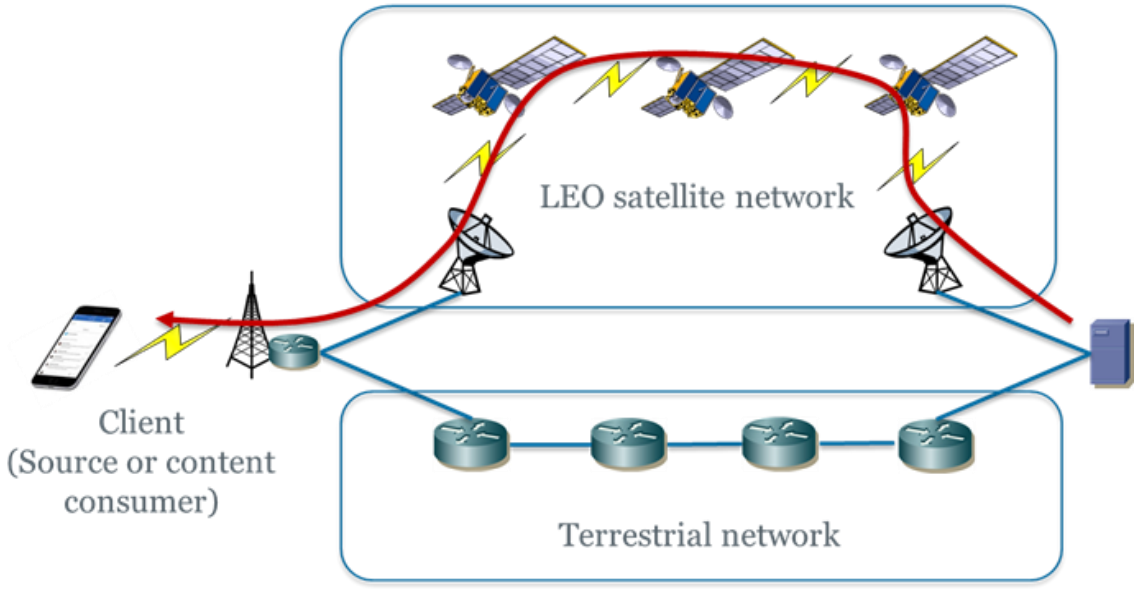


Figure 37- Decoupled Scenario

11.3.2 Coupled scenario

One typical design rationale behind this scenario is the uncertainty on the readiness of inter-satellite links based on laser commutations. Without the availability of such links, one typical scenario will be the one

that is shown in **Figure 38**, where each LEO satellite is integrated with the terrestrial infrastructure on per-hop basis. As such, it is not applicable to run any dedicated routing protocols directly between satellites, but instead each satellite is supposed to be an integrated component of the overall framework on the ground running common routing protocol. Another view can be that, the introduction of these satellites offers the opportunity to create "shortcut" paths compared to BGP routes across domains. Another key difference compared to the decoupled scenario is the role of downlink/uplinks between satellites and the ground infrastructure. From **Figure 37** it can be seen that such links in the decoupled scenario are only for access purpose, while in the coupled scenario such links will take both roles of access and transit, in which case the bandwidth capacity needs to be adequate for such purpose.

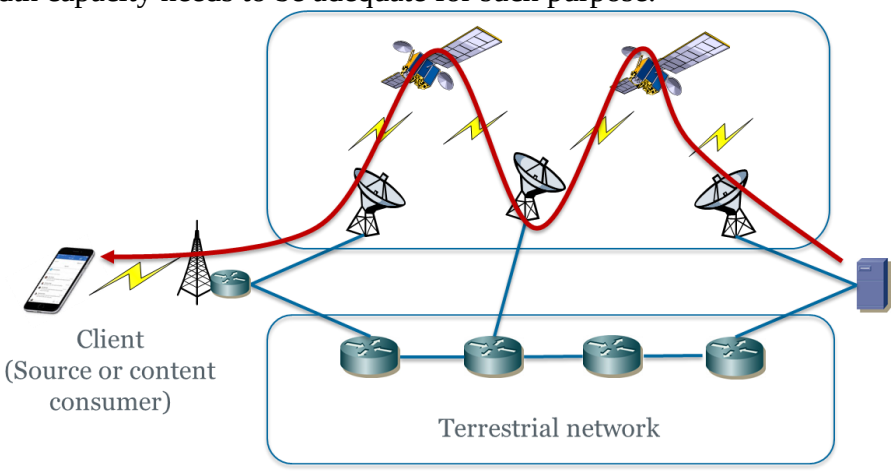


Figure 38- Coupled Scenario

11.3.3 Using LEO satellites as access network

The benefit of using LEO satellites to provide access service is mainly due to its ubiquitous access coverage, even at rural areas such as oceans, mountain for desert areas where it is difficult or even impossible to deploy any fixed infrastructures. A typical use case can be described as follows. Passengers on a cruise ship in the Atlantic Ocean would like to watch video content offered from a content provider in mainland Europe. Today's scenario is to equip satellite dish on the ship and internally use onboard WiFi to provider Internet connectivity to them to reach the content source or CDN node. In the future individual users onboard can directly use their individual mobile devices to access Internet through the LEO satellites that has the local coverage of the area. While the last-mile access is already provided by LEO satellite, in order to stream video content from the data centre on the land, still it is necessary to build a content delivery path from the content source to the users, involving either completely a chain of LEO satellites, or a combined path consisting of both terrestrial routers and LEO satellites (**Figure 39**).

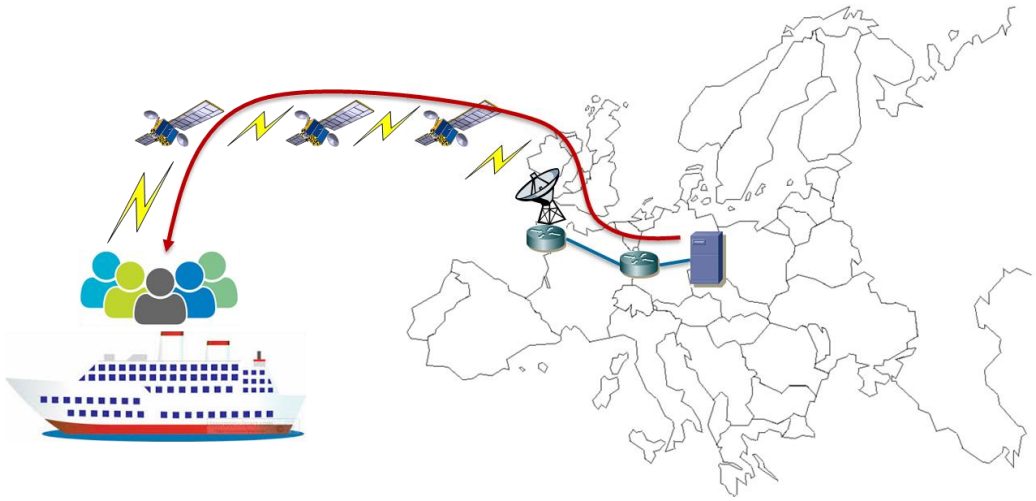


Figure 39-. LEO satellite for access service

11.3.4 Design options on addressing and routing

In this section, we address basic networking challenges on the integration of space and terrestrial network infrastructures including addressing and routing paradigms. It is worth noting that routing optimization across LEO satellite networks have been extensively studied in the literature, but how to seamlessly harmonize or even unify the routing infrastructures between the two types of networks have been much less investigated, and below we highlight three different strategies.

11.3.4.1 Design option I – Incremental adaptation on BGP with legacy IP addressing

First in this option, the strategy is to directly apply the legacy IP paradigm to the space network. That is, both the space and terrestrial network would use IP addressing and routing under the same manner. This option can be seen as a relatively conservative scheme. The benefit of adopting such option is that the current well developed advanced terrestrial applications can be natively supported also in the space network. However, due to the constellation behaviours, the space-terrestrial link can be very unstable, which will lead to potential problems such as frequent and simultaneous link broken events, routing protocol convergence difficulty. For example, considering the scenario shown in **Figure 40**, where the IP address is binding to the interfaces of the devices. As can be seen from the figure, router 1.1.1.1 is currently connecting to satellite 1.1.1.2 and will connect to satellite 2.2.2.2 for the next time period due to constellation mobility. Considering the IP addresses are static configured and most of the IP routing protocols rely on these addresses to build their neighbours. As a result, after the mobility event the routing protocols of both ends will lose their neighbours, because the IP addresses are miss-matched (i.e., the two direct-connected devices are now in different network segments).

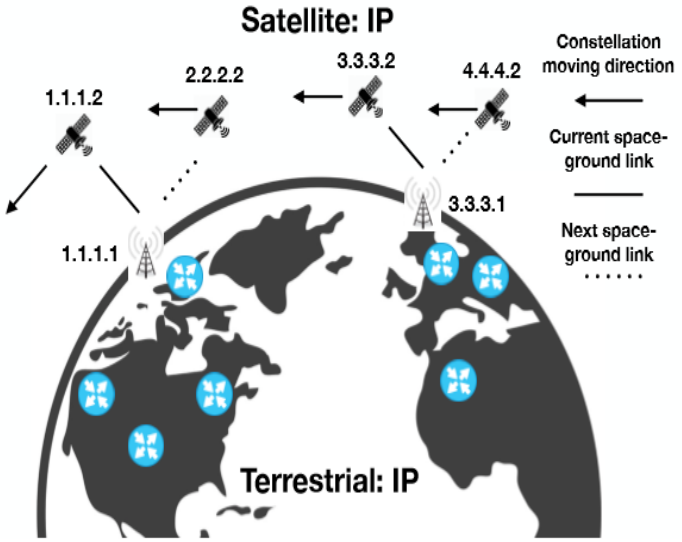


Figure 40-. Envisioned addressing and routing system in option I

Thus, the relative infrastructure mobility between the space and terrestrial network is certainly one of the key features to be investigated and some preliminary studies within this family (i.e., applying IP routing principles in LEO satellite networks.) has recently been carried out with the consideration of constellation behaviours. For example, in [2], a brief study of applying BGP directly in the satellite network is provided and the results indicate that up to 45% available satellite connectivity is wasted due to the unstable eBGP session. To address such issue, in [3] a scheme named NTD-BGP is proposed aiming to preserve the eBGP sessions between the space and terrestrial routers in the mobility events. However, it has difficulty in fitting the inter-AS scenario where the terrestrial router is moving into a new satellite AS while NTD-BGP requires the BGP speakers to always establish the eBGP session using a fixed loop-back address. Thus, if the dedicated loop-back address is not advertised to the new satellite AS, the eBGP session is then unable to be established.

Apart from the traditional static IP address configuration, dynamic address configuration may provide us another thread. For example, by utilizing relative fixed geography information such as longitude and/or latitude, the IP addresses can be bound to predefined regions instead of the router/interfaces. Thereby, from the terrestrial router's point of view, IP addresses of the space peers become stable. However, such addressing scheme could lead to the convergence problem of IGP/iBGP within the space network domain. One potential strategy is to proactively calculate the routes and store the result for future use. The feasibility of this strategy is based on the fact that the satellite behaviour is almost predictable.

In summary, applying the existing IP technology in the satellite network can preserve the current IP ecosystem to the largest extant. However, developing effective methods to restrain the dynamic-topology issues caused by satellite-terrestrial mutual mobility is required.

11.3.4.2 Design option II – Separate routing with protocol translation based on alternative addressing system in the space network

In this option, the strategy is to keep the existing IP system for the terrestrial network, meanwhile, to design an enhanced addressing and routing system for the space network. This is relatively more radical compared to the previous option. Such option will involve a development of a set of new technologies within the space network domain, thus a foreseeable higher cost is needed compared to the first technology option. However, considering the new techniques are to be deployed in the space network where the deployment of the addressing and routing is still at its very early stage, such an option would therefore receive less stress from the deployment side. Nevertheless, the new tailored space network addressing, and routing

architecture should still face technical challenges from the space-terrestrial compatibility problem. Ideally, the new architecture should not interfere the network behaviours of the terrestrial network. Moreover, the new addressing and routing system should be able to bypass the aforementioned satellite-terrestrial mutual mobility issue, i.e., the new system should have excellent mobility support for the accessing terrestrial networks. In **Figure 41**, we depict the space-terrestrial networking system under this option. Since the addressing and routing systems in the space and terrestrial networks are different, the mutual mobility issue is bypassed because the two networks cannot recognize the topology changes of each other. However, in this scenario, protocol translation is required to assist the packet forwarding across network boundaries. From the terrestrial network's point of view, once the IP packets reach the space-terrestrial border, they will be encapsulated with the satellite network addresses and transmitted to another space-terrestrial gateway. As a result, the satellite network is seen as a tunnel for the terrestrial network as IP is not involved in the satellite network. In such case, the IP applications initiated from the space network would not be natively supported unless auxiliary functions are introduced. The latest research work [2] has proposed the path-aware network framework to integrate the LEO satellite with the fixed Internet. In the context of [2], the availability of a satellite-ground link is exchanged among terrestrial ground stations and such information is provided to end-devices for path selection. The authors propose to encapsulate an additional IP header to the normal IP packets to indicate the preferred source/destination terrestrial ground stations and then use the LEO satellite network as the backbone network (similar to the scenario described in section 3.1) to build a tunnel between the terrestrial ground satellite for long distance communication. Such a design has achieved the following properties: low impact to current system, cost-efficiency in deployment, low latency in long distance transmission. On the other hand, the solution still requires tunnels as an auxiliary mechanism for the end-to-end data delivery. Meanwhile it still remains an open issue whether such a solution is able to support both scenarios of using LEO satellites for backbone as well as direct access for end users.

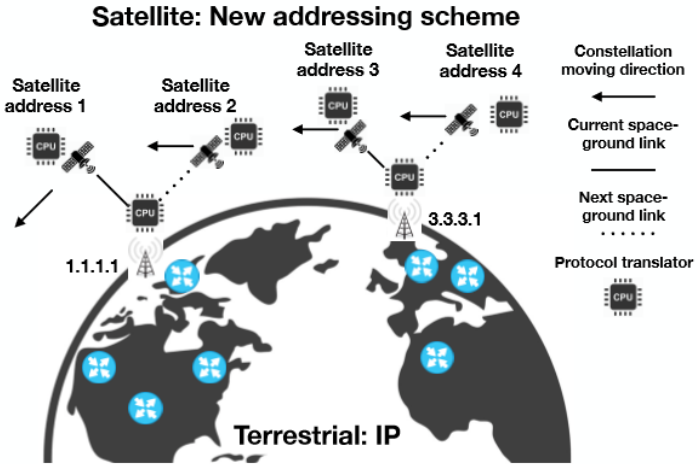


Figure 41-. Envisioned addressing and routing system in option II

11.3.4.3 Design option III – Unified addressing framework allowing flexible routing in space and terrestrial networks

In this option, the strategy is to design a comprehensive integrate addressing and routing system for both the space and terrestrial networks. Apparently, this is the most radical option among the three proposals. The new addressing and routing system in this case should be able to natively overcome the issues caused by the topology dynamics, this includes the dynamicity within the satellite constellations and between the space-terrestrial links. The ultimate ambition of this option would be to integrate any network especially

future network architectures, rather than restricting to legacy IP-based networks. Therefore, for this option, the requirement for compatibility, scalability, robustness, and mobility support should be satisfied from basic design. Although developing such a new architecture can be very challenging plus it will also face significant pressure from the deployment side as there may be strong impact on the current network system, the reward can be potentially significant. Compared to option II, the most prominent benefit is that, end-to-end communication is natively supported (rather than requiring tunneling or protocol translation between the networks) since the space and terrestrial networks are running the same addressing and routing framework. To achieve this goal, any method is open for discussion, this may include but not limited to introducing additional fields in IP packet headers and/or routing tables, or even location-free schemes. In **Figure 42**, we depict the envisioned space-terrestrial networking system under this option. As can be seen, both the space and terrestrial networks are running the new designed addressing and routing system, in which the integrated address may contain information from multiple protocols. In principle, the routing in the space should simultaneously take into account both the satellite address and the IP address instead of completely relying on satellite address by encapsulating the IP address, as is the case in Option II. Thereby, the user devices running on legacy IP can freely switch their connections between the space and terrestrial network depending on the network performance. As such, advance internet services such as caching, video accelerator can also be supported in the satellite network. Finally, it is worth noting that, since there is no packet header encapsulation in this case, when a packet is being delivered through the terrestrial network, the header field for satellite address can be either reserved for other purpose or eliminated with mechanisms such as variable-length IP addressing schemes.

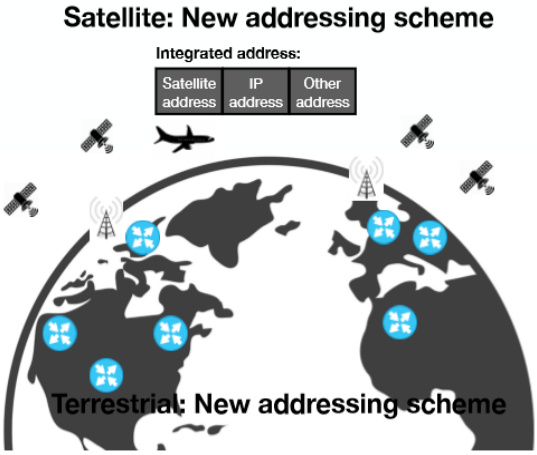


Figure 42-. Envisioned addressing and routing system in option III

11.4 Other Advanced Functionalities and Features

11.4.1 Supporting of unicast, multicast, broadcast and anycast

In addition to the support of the basic unicast function, the LEO satellite network should also support other advanced modes of communication including multicast/broadcast and anycast. Concerning multicast, a key challenge is the stability in maintaining the multicast tree against the dynamic change of the LEO satellite network topology, in particular concerning the establishment and tear-down of transient network links between encountered LEO satellites that belong to different constellation orbits, in which case the maintenance of the link can only last for a short period of time. If the multicast tree consists of network elements on the ground, then the stability issue of maintaining the multicast tree will also involve necessary handover between LEO satellites and the terrestrial infrastructure such as ground stations. The same technical issue is also applied to the anycast scenario in terms of maintaining the connection with the

targeted content/data source.

11.4.2 Access/admission control and security

Due to the relatively limited communication resources in the space as compared to the terrestrial network infrastructure, access and admission control mechanisms need to be in place in order to avoid excessive or non-authorized user traffic to be randomly injected into the LEO satellite network. Traditionally, such functionality can be fulfilled by the facilities on the ground, e.g. ground stations which are interfacing the satellites. However, in the future if each satellite is able to provide direct communication link with end user devices without necessarily going through ground stations, then each LEO satellite, acting as an access router, should be able to take the responsibility of access/admission control in order to protect the network resources on the satellite network side. To generalize this, further security mechanisms and functionalities (e.g. firewalls etc.) can be also deployed on the LEO satellite network side.

11.4.3 Edge caching and computing

The current vision of the LEO satellite network has mainly focused on the simple data delivery function. However, there have been some initial feasibility discussion on the capability extension to support edge-based content caching and computing thanks to the relatively short latency in such an environment compared to the GEO satellite scenario [4]. In this case, each LEO satellite will need to be equipped with lightweight computing and data storage facilities in addition to simple routing and forwarding. On the other hand, the corresponding technical challenges mainly include: (1) Limited power/energy supply to maintain the normal operation of computing facilities; (2) potentially higher data error rate due to space magnetic radiation on storage media; (3) frequent handover between LEO satellites and the ground infrastructure which leads to potential service stability issues.

11.4.4 Network slicing

In the context of 5G, network slicing [5] has been deemed as a promising feature for operators to provision network resources and functions in order to tailor for heterogeneous requirements of emerging applications and services. While the business model for network slicing on the traditional network operator side has been relatively clear, a more complex scenario of involving satellite operators has not yet been previously elaborated. As a starting point, a terrestrial network operator can rent virtual network resources provided by a satellite operator in order to build a dedicated backhaul link for connecting its point of presences (PoPs). In this case the terrestrial network operator is able to create end-to-end slices for supporting different application types, and the backhaul component of selected subset of slices (e.g. eMBB (Enhanced Mobile Broadband) for video content delivery) can leverage on the satellite capability.

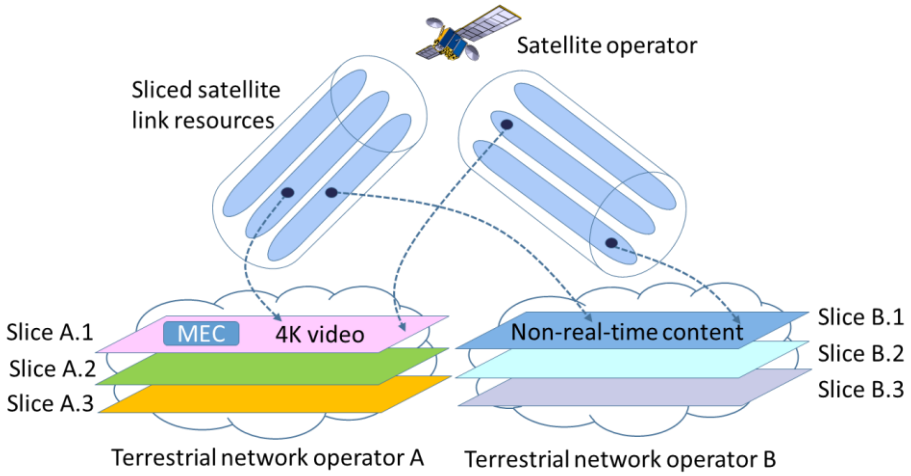


Figure 43-. Business scenario for network slicing

On the other hand, a satellite operator could also slice its own satellite link resources and lease to multiple terrestrial network operators for backhauling or extended access services, in particular by applying intelligent beamforming techniques to cater for different geographical areas. As shown in **Figure 43** (for simplicity only one satellite is shown but it can be a chain of LEO satellites), sliced satellite link capabilities can be lease to terrestrial network operators (e.g. mobile operators) in order for them to build own service-tailored slices provided that the sliced satellite capability is able to fulfil the targeted service requirements. For instance, in the **Figure 43** once terrestrial network operator A has deployed a MEC-based content prefetching/caching network function within its network slice (Slice A.1) for transmitting 4K/8K video content, then it can use leased satellite capability for backhauling 4K/8K video in that slice. From the business point of view, we can envisage a cash flow from end customers (subscribers of terrestrial network slices) to the terrestrial network operators and further to the satellite operator.

11.5 Implication to Key Network Management Operations

We briefly discuss the network management implications from the viewpoint of the following major features.

- *Traffic engineering (TE).*
  Network traffic engineering has been well investigated for more than two decades in the context of traditional terrestrial Internet. However, TE has not been systematically understood in the integrated space and terrestrial network environment, specially giving the district characteristics of the two types of networks and also the mega-constellation behaviors of LEO satellites. It is generally understood that the inter-satellite link capacity is not compared to the optical fiber links in the terrestrial Internet. As such, the traffic injected into the space network has to be selective. Policies can be enforced either based on the traffic type and their QoS requirements, or based on other contexts such as the distance between source and destination pairs. For instance, in [1] it has been argued that routing through a chain of LEO satellites will outperform the usage of terrestrial Internet in terms of end-to-end delay if the distance of the source and destination is beyond 3000 kilometers. It is also worth noting, the capability of TE in the space network also largely depends on the specific routing mechanisms that are deployed, which has been the case of terrestrial network environments, e.g. IP/MPLS/SDN.

- *Quality of Services (QoS)*
  In theory, the introduction of the new capabilities from the space network should be able to improve QoS and resilience offered from the terrestrial network infrastructures. However, without systematic network engineering solutions, QoS/resilience requirements will not be automatically met in practice. First of all, at the service management level, how to establish provider-level service level agreements

(SLAs) that include QoS and resilience requirements can be negotiated between the terrestrial network operators and space network operators needs to be investigated. Secondly, in order to enforce the actual QoS-awareness (e.g. end-to-end QoS-constrained paths), routing optimization, resource allocation and traffic admission control mechanism need to be in place, especially by taking into account the constellation mobility of the LEO satellite infrastructure which may cause stability issues.

- *Resilience*

The traditional fault management paradigms for network resilience will also be expanded to cater for the new challenges (and also opportunities) introduced by the space network. Specifically, it can be envisaged that the two types of networks can be complementary in protect each other in terms of failures or anomalies. For instance, in case a terrestrial network part suffers from failure, the effected traffic can be diverted to the space network in order to avoid traversing the failed component and vice versa. Generally speaking, there are two technical challenges pertaining to fault management which can be well applied here: 1. *Fast failure recovery* – how to seamlessly re-direct traffic to backup network capabilities so that end users will not be able to perceive any service disruptions caused by the transient loss of connectivity. 2. *Post-failure network/service performance* -
How to maintain the originally targeted QoS assurances and network performances (resource usage) even after failures take place and cannot be restored in short term.

12 Routing and Addressing

Routing protocols have been key components in networking technologies, and continuous developments and evolutions of routing protocols are essential to provide better network services which are the foundations and building blocks of new applications and services. This section focusses on new requirements of routing protocols for NETWORK2030. Section 12.1 brings up few high precision services requirements of routing protocols in access, edge and core networks of NETWORK2030 for both intra and inter-domain routing protocols. Section 12.2 introduces a few emerging routing protocols that are being developed.

The routing requirements for NETWORK2030 are based on the services and use cases outputs from sub-groups 1 and 2. **Figure 44** is a summary of the requirements and goals.

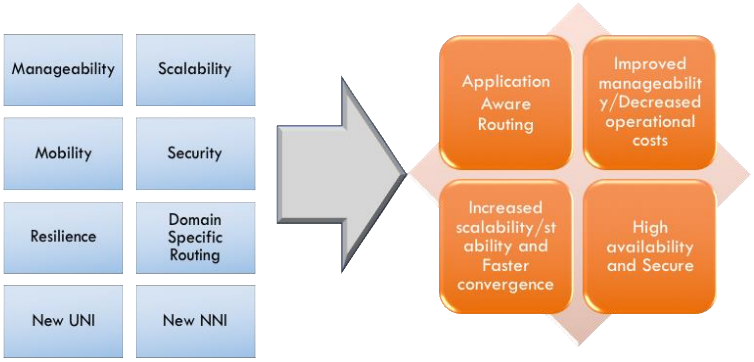


Figure 44-. Routing protocols requirements and goals for NETWORK2030

12.1 Routing Requirements in Network2030

Routing protocols play a significant role in today's networks and have evolved over the years to meet the ever-changing requirements of the Internet. Currently the most commonly used routing protocols include OSPF, IS-IS and BGP. With the new developments and use cases envisaged by NETWORK2030, existing routing protocols need to be enhanced, and new routing protocols will potentially be required to meet the new requirements from different perspectives.

The followings are a list of routing challenges that need to be considered for NETWORK2030:

12.1.1 Path and Topology Policies

When choosing best paths or topology structures, the following criteria should be considered:

- How a path or path set is calculated, e.g. a path can be selected automatically by the routing protocol calculated best path or imposed by a central entity, for example for traffic-engineering reasons.
- What criteria are used for selecting the best path, e.g. classic route preference, or administrative policies such as economic costs, resilience, security, and/or geopolitical considerations.

RSVP-TE [ROUT.10], is widely deployed and establishes paths using Explicit Route Objects (EROs) with or without bandwidth reservation. RSVP-TE does this by introducing per-path, per-hop state, with some control plane overhead (slow hop-by-hop per-flow state processing signalling mechanism) and lower scalability. Segment Routing (SR) [ROUT.11] proposes to replace RSVP-TE.

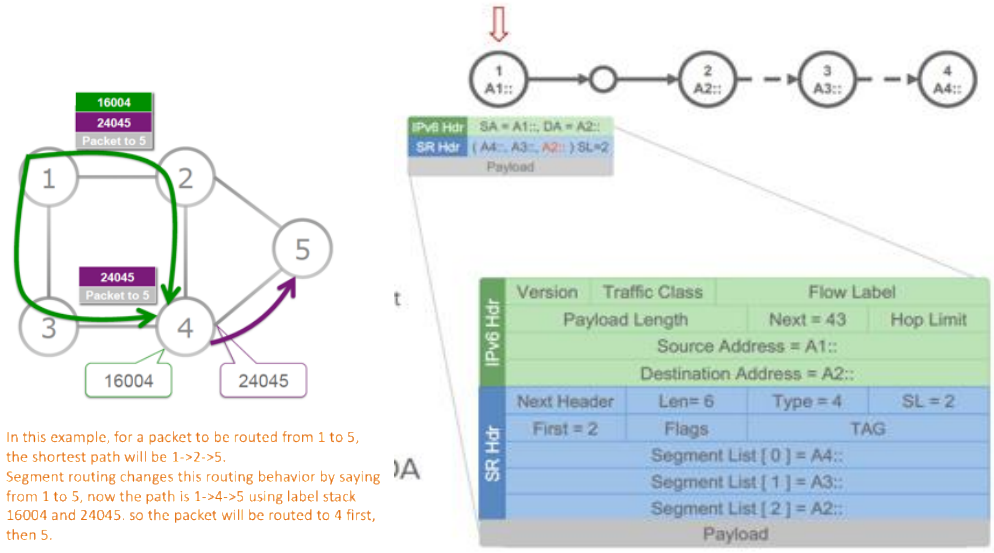


Figure 45-. Segment Routing

While Segment Routing (SR) technology supports packet steering from the source by using instructions (SIDs) included in the packet it does not support high-touch per-path hop-by-hop functions such as monitoring, accounting, QoS (Policing, Shaping, Buffering) or other processing. In the case of a link or node failure, SR proposes to use Topology Independent Loop-free Alternate ((TI-LFA) [ROUT.12]. This makes the repair path congruent with the post-convergence path in order to minimise the formation of micro-loops. IP fast reroute (IPFRR) techniques such as TI-LFA aim to provide protection of SR, LDP and IP traffic in sub-50 ms [ROUT.13], and this may not be good enough for future applications with high precision requirements [sub-group2 doc ref]. However, the TE characteristics of the SR path may not be preserved if a link/node failure along the TE path as TI-LFA can only compute a loop-free shortest path from the point of failure, as opposed to matching TE properties of the SR path. **Figure 45** illustrates how SR works.

TI-LFA is only one of a large number of IPFRR techniques that have been designed [ROUT.14] and only one approach to avoiding micro-loops during reconvergence [ROUT.15]. This is an active area of work and new techniques continue to be proposed for example [ROUT.7].
Additionally, new approached to path construction in routing networks continue to be researched such as PPR-Path [ROUT.6] and PPR-Graph [ROUT.8].

This mixed approach PPR of centrally computed TE paths or graphs (point-to-multipoint) based on the characteristics alluded above but responding to dynamic routing events in a distributed fashion would be useful to cater the high-precision service demands [Sub-Group 2.1, Sub-Group 2.2]. These paths and graphs should provide some of the QoS characteristics in the steady state as well as in FRR cases by responding to local link/node failure detection. To maintain the service level objectives, any failure detection should not resort to shortest-paths or a slow ingress detection/switchover technique, which can potentially cause high-precision service disruption [ROUT.7]. If the underlying dynamic routing protocol were to provide these services, it is essential to maintain the convergence properties for the regular shortest-path routing in the network (for best-effort traffic).

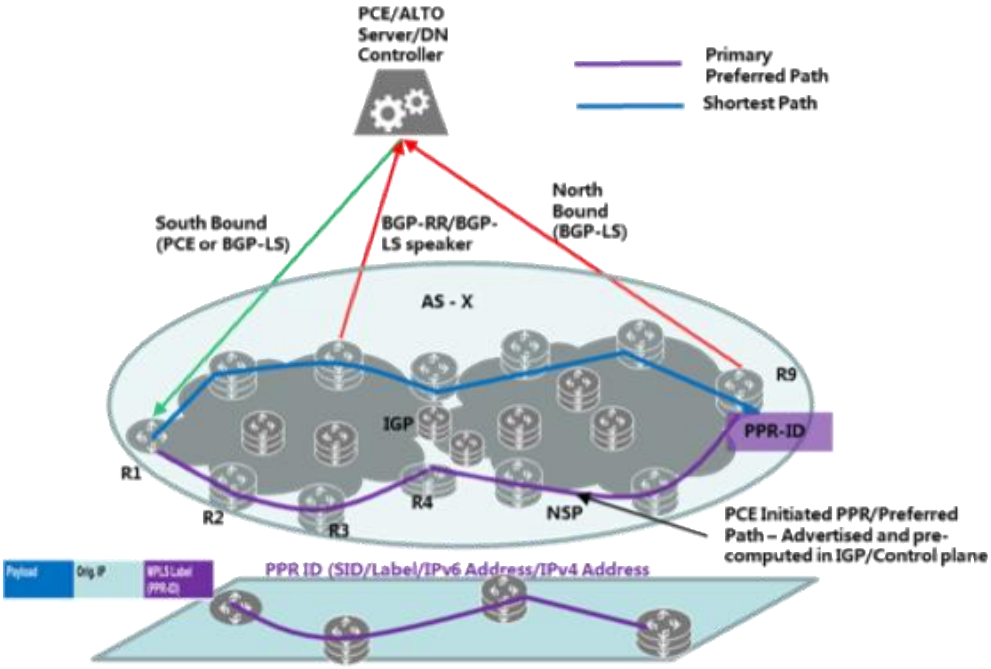


Figure 46-. Illustration of Preferred Path Routing (PPR)

12.1.2 Predictive Routing

Predictive routing means the change in the state of a router/host can be predicted; hence the routing algorithm can make route changes before or as an event occurs. There are new categories of applications that may benefit from predictive routing: such as with cars driving on a highway, or robots moving in a factory. These are applications where packet loss or delay is potentially very harmful, but their movement can be either pre-defined or predicted in a way.

An alternative approach that alleviates the effects of slow routing protocol convergence is embodied by protocols with packet-carried forwarding state, such as SCION [ROUT.16] or Segment Routing [ROUT.11]. In such protocols, forwarding information that is carried in the packet header does not rely on router's (inter-domain) forwarding tables, and thus avoiding inconsistent forwarding table state due to asynchronous update mechanisms. Moreover, the nature of the path exploration process in SCION (referred to as beaconing) which creates path segments, does not require any convergence for connectivity -- instead, additional paths are created over time that become available. Basic end-to-end connectivity, however, is established based on the initial path segments that are disseminated.

In general, the network infrastructure is fixed subject to the impacts of failure, maintenance and upgrades. However, there is a new class of network emerging based on the use of mobile network infrastructure components such as large constellations of low orbiting satellites. These have the property that whilst the network infrastructure is dynamic, and the best paths are constantly changing the best path is predictable some for some considerable time. This allows a new approach to routing based on current knowledge of the future disposition of the infrastructure rather than on preconfigured “static” paths, or dynamically discovered paths.

12.1.3 Domain-Specific Routing Protocols and Algorithms

New routing protocols are being developed in the IETF for data centers, e.g. RIFT and LSVR. These are protocols specifically optimised for use in certain types of domain and topologies. Such protocols trade

general applicability for high performance in the target domain. Soon, there could be more domain-specific cases that require new routing protocols or algorithms, such as routing for satellite communications.

12.1.4 Industrial Internet and Internet of Things

Industrial internet refers to the interconnected networks of sensors, robots etc. Internet of Things (IoT) network consists of control systems, embedded systems etc., and in consumer market, IoT is essentially the technology to build smart home and smart cities, and enable applications including healthcare, disaster recovery etc.

New technologies and standards are being developed at a rapid pace to form different IoT ecosystems and networks. From routing perspective, the typical common requirements among these networks are:

- Low power consumption. Typical IoT devices are powered by batteries with limited processing power and memory, and this means they need to be conservative on power consumption when sending data packets or control packets. Routing protocols designed for such IoTs should be quiet without sending too many control packets, and then resulted data packets should not have big encapsulation header.
- High availability. Applications such as disaster recovery requires the network to provide non-disruptive service in case of network failure, power outage and natural disaster etc.
- Mobility. IoT devices should be able to connect and communicate with the network or other devices without location and access technology limitations, whenever and wherever.
- Large number of connections. The number of various IoT devices to be connected to the network will be in thousands or millions, so routing protocols are required to connect these huge number of heterogeneous systems.

There are two key issues that future network designers need to contend with in IoT networks. Firstly, the high path quality needed, which requires the routing system to establish the path and allocate the resources, including the case where it may need to configure the network to strategically replicate and eliminate packets to maximise their chances of successfully traversing the network [ROUT.17]. Additionally, many IoT devices are designed to meet extreme physical size, cost and lifetime power budgets. The protocols that these devices use require extreme regard to resource conservation and may not be able to use the "standard" network protocols which are optimised for characteristics such as generality and performance.
.

12.1.5 ManyNets and Routing in the space

While there is no relation between wireless mesh network routing challenges and protocols developed in IETF MANET WG, Routing in space with LEO satellite constellations presents domain specific routing challenges.

In a system, where complete global connectivity is provided through LEO satellites, which includes inter satellite connectivity using Free Space Optical (FSO) transmission, introduces unique set of challenges w.r.t routing in space and possible traffic engineering [ROUT.1]. This is because (as noted earlier) of the continuous changes to the network paths as the nodes in the orbit are on the move. There is no routing protocol today which does shortest path computation when all the nodes in the network are continuously moving. However, one characteristic of this network is the movements of satellites are completely predictable and this can be factored for new route computation methods. This also introduces unique set of Fast ReRoute (FRR) challenges which are not applicable for terrestrial networks. However, it is worth noting, at this time the applicability and possible deployment of such a system is constrained by free space optics (FSO) limitations. These limitations concern with the inter satellite link capacity, which is currently in the order few Gbps [ROUT.18] [ROUT.19], while the sub-sea fibre optical cable provides bandwidth in the order of 10's of tbps.

The resulting low-Earth-orbit (LEO) constellations will not only bridge the digital divide by providing service to remote areas, but they also promise much lower latency than terrestrial fiber for long distance

routes. Unlocking this potential is non-trivial: such constellations provide inherently variable connectivity which today's Internet is ill-suited to accommodate. In fact, the use of the BGP protocol to integrate the satellite network in today's Internet unfortunately encounters several major challenges:

- The highly dynamic nature of ground station to satellite links creates
- Scalability limitations for BGP, especially due to weather disruptions;
- During early phases of deployment, connectivity will fluctuate so often that slow routing convergence with BGP could make the partially deployed constellation unusable;
- The higher cost and lower bandwidth of satellite network links complicates their use for all data traffic, thus complicating the management of differentiated traffic.

There have been proposals to address these challenges. Giuliari et al. propose an optimal solution based on the SCION path-aware-networking architecture, and given this clean-slate baseline, they then develop a more pragmatic solution based on a CDN-like architecture [ROUT.20].

12.2 Network layer UNI and NNI

Routing protocols have previously been based on the calculation of best/shortest paths in terms of a single metric – a relatively static calculation as these metrics do not change other than in response to operator configuration. Currently most Traffic Engineering path computations that take into account current network load and resource availability use relatively stable metrics and are a simple variant of best path computations, and researches are being done to apply machine learning to networking and to calculate more complex paths. NETWORK2030 will demand the consideration of new factors during path calculation, such as network resources (bandwidth, storage etc.), dynamic traffic distribution, service location, link and node resilience, delay, jitter, and loss. Many of these factors may need to be considered at the same time.

Based on the requirements from applications, routing protocols should be able to provide a path or a set of paths that satisfy the requirements, such as going through a specific router for a policy or a service or to meet a minimum bandwidth requirement.

User-network interface (UNI) is between end-user device and the service provider. It is responsible for the message exchange about the service requirement information, which includes:

1) User Service Expectation: It is the message from end-user device to the service provider to describe user's expectation in network service, such as Maximum/Minimum bandwidth required, maximum latency, etc.
2) Path Quality Information: It is the message from service provider to end-user device to notify each path's network quality parameters, such as maximum/minimum bandwidth for a direction, maximum latency, etc.
3) Path Segment Information: It is the message from service to end-user device to notify each path's network segment parameters, such as path index and associated list of segments (IP addresses or MPLS labels).
4) Data Plane Information: It is the message from service provider to end-user device to notify end-use to send data by the specified data plane, native IPv6, SRv6, MPLS or other encapsulations.

A UNI interface could be a newly defined protocol, or through the extension of existing protocols, such as DHCPv6 or IPv6 Neighbour Discovery.

External Network-network interface (ENNI) between two networks is responsible for the message exchange in order to support end-to-end services. The information includes:

1) Path information that may contain path segment info or how to route packets.
2) Path Quality Information that is a path's network quality parameters, such as path index, maximum/minimum bandwidth for a direction, maximum latency, etc.

ENNI interface could be a newly defined protocol, or through the extension of existing protocols such as BGP.

12.3 Mobility

Mobility needs to provide ubiquitous connectivity to mobile users, independent of type and location of devices, access technologies etc. A mobile node must be able to continue to communicate with others when access location or technology changes when moving and still providing efficient content delivery and trustworthiness.

There have been researches and proposals on mobility for years. One current approach to mobility issues, is that they are resolved by the applications themselves using technologies such as MPTCP, QUIC (https://datatracker.ietf.org/doc/draft-ietf-quic-transport/), etc. at the transport layer. Another approach is the Mobile Ad hoc Networks (MANETs) [https://datatracker.ietf.org/wg/manet/about/], which is to provide a network layer solution to support node motions, including IP routing protocol functionality suitable for wireless routing applications.

For the Internet of Everything (IoE) the collaboration of IoE based devices with current 1Internet protocols is challenging, specifically in terms of mobility and scalability.

Mobility scenarios in cellular networks pre-REL15 [ROUT.21] involves only access layer i.e., UE's mobility from one NodeB to another NodeB with same or different Mobility Management Entity (MME). However, 3GPP REL15 [ROUT.21], presents various mobility scenarios which involves IP address changes with or without service continuity as described in various Session and Service Continuity (SSC) modes. In the scenario, where IP address change causes disruption to session continuity, to maintain service continuity, various solutions are specified in [ROUT.21], involving changes to transport layer protocols at UE. While other category of such solution involves network assisted service continuity with multiple PDCP sessions and stitching these sessions in backhaul network to prevent the services interruption at the UE without any or with minimal packet loss.

However, there are not widely accepted/deployed solution in network layer yet for new service requirements described in FGNETWORK2030 SubG2. With the development of new applications in NETWORK2030 with uRLLC requirements, it is desired to support mobility in network layer, which avoids the session interruption and minimizes the packet loss and latency.

12.4 Routing Security and Resilience

Ensuring the security of routing mechanisms continues to be a challenge. Routing attacks include route-hijacking, i.e., diverting traffic to an adversary-controlled domain, and denial-of-service
attacks exploiting the routing mechanism, i.e., preventing communication. Over the past four decades, numerous researchers studied secure routing in a variety of network types and settings.
We briefly highlight the core challenges and several proposed approaches.

An overview of routing security is available as a taxonomy for secure routing protocols by Hollick et al. [ROUT.23], which emerged from a recent Dagstuhl seminar on secure routing [ROUT.24]. The taxonomy establishes the following general services that need to be protected: identity service, routing service, topology service, and transport service. An adversary can have a variety of capabilities, resources, and goals -- the security section lists different categories of capabilities and resources as defined in Section 7

of this document. In the context of routing, the main goals are to violate the following security properties: availability of routing and forwarding, authenticity of routing information, confidentiality / privacy of routing and topology information, and anonymity of entities (e.g., mobile users could be located via the routing protocol). In terms of security properties of the forwarded packet data, the routing system should prevent the re-direction of traffic flows through entities that intend to eavesdrop or alter packet traffic -- if communication is already passing through a malicious entity, it is the responsibility of the data plane to ensure traffic secrecy and integrity.

Routing protocols, especially IGPs, have been running in a relatively benign environment. With the development of new applications, it is critical for the network to provide non-disrupted service especially to high value traffic. Also considering more hosts/IOTs are being added to the network, security is becoming more and more critical.

Secure intra-domain routing protocols have been largely neglected compared to inter-domain settings, as one assumes a benign environment under single administrative control in these settings. In existing intra-domain protocols, however, adversaries can launch several attacks: availability, denial-of-service, or traffic redirection. The typical approach for securing link-state intra-domain routing protocols is to attach a cryptographic signature to link-state updates, as is done for instance in secure OSPF. Within a single administrative domain, the entity identification problem is simplified, as the network administrator can establish and distribute cryptographic keys and certificates among networking devices and systems.

Inter-domain secure routing continues to be a challenge up to today. While S-BGP and its successor BGPSEC have been developed over the past 20 years, they have seen limited deployment due to several reasons: worse scalability than BGP (due to the inability for prefix aggregation and the need for periodic dissemination of routing updates), operational challenges (obtaining and handling certificates, updating router software and possibly even hardware), limited security benefits (new attacks are made possible), slower convergence than BGP, and disruption of policy mechanisms (ASpath alteration / prepending). A beacon of hope is the resource public-key infrastructure (RPKI), which provides the prefix and AS certificates in BGPSEC, as it enables route origin validation, which is easier to deploy than full BGPSEC and in itself addresses several attacks [ROUT.22]. Unfortunately, the RPKI introduces a circular dependency with routing, as route message
verification requires RPKI certificate validation, and RPKI certificate validation requires a route to a server to fetch the RPKI certificate database [w]. Moreover, the RPKI also opens up vulnerabilities to misbehaving RPKI authorities, where a misconfiguration or malicious action can result in rendering an address range unreachable [ROUT.25].

It appears that an Internet re-design is needed to resolve the thorny issues to secure BGP. The SCION [ROUT.16] secure internet architecture has thus re-designed the routing and PKI infrastructure from ground up to achieve high levels of security [ROUT.26]. By avoiding inter-domain forwarding tables on routers and utilizing a path exploration system that does not rely on convergence, many attacks and vulnerabilities are prevented by design. The control-plane PKI in SCION is constructed such that the distribution of cryptographic credentials follows the transmission of routing messages, thus avoiding circular dependencies between routing and certificate distribution. The definition of trust
roots within each isolation domain ensures operational sovereignty and prevents external entities to affect operation due to misconfigurations or misbehavior. As a consequence of its design, SCION can prevent all known routing attacks.

Current routing protocols are built and operated on the assumption of a high degree of trust. IGPs are typically running within a controlled, and secured domain, and BGP connected with trusted neighbours. For NETWORK2030 there are three possible solution directions (not exclusive of each other):

- Making existing routing protocols more secure by adding new authentication mechanisms/algorithms etc.
- Securing and authenticating the information distributed by routing systems (such as by RPKI mechanisms applied to BGP – ref SIDR)
- Using a new secure routing protocol, e.g. SCION.

In case of link or node failure, routing protocols should be able to continue to provide an acceptable level of service. This could be achieved through local repair techniques, such as Loop-Free Alternate (LFA) Fast Reroute (FRR) [ROUT.14] [ROUT.15]. Meanwhile routing protocols should re-converge fast and bring the network back to a stable state.

Mutually Agreed Norms for Routing Security (MANRS) [ROUT.27] is a global initiative, supported by the Internet Society, to provide crucial fixed to reduce routing threats.

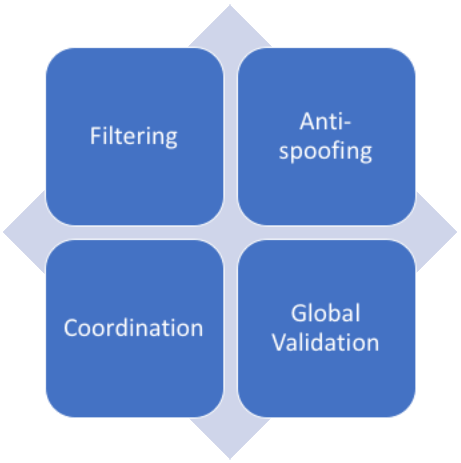


Figure 47-. Proposed actions for service providers by MANRS

- **Manageability and easy operation**

Easy configuration and debugging. Currently, network management focuses mainly on single devices. This will become harder and more costly as the number of devices in the network keeps growing. Future routing protocols should support Zero Touch Provisioning (ZTP), and real-time state notifications to facilitate control plane telemetry. Enhancements to existing protocols could be done to easy configurations.

- **Scalability**

With IoT, the number of connected devices is already at billions and is expected to continue to grow. It is common for a Data Centre network to have more than several tens of thousands of end points.

Need to address the scalability of “scale down” here. Such as for devices with limited power supply that can only transmit limited amount of data

12.5 Emerging Routing Protocols

- **RIFT**

RIFT (Routing in Fat Trees) is a novel routing protocol defined by IETF [ROUT.30]. It mainly targets Clos [ROUT.28] and fat-tree network topologies based data center, and is optimized with minimization of configuration and operational complexity.

RIFT is mixture of both link-state and distance-vector technologies and can be described as “link-state towards the spine” and “distance vector towards the leaves”.

Here are the major characteristics of RIFT:

- Northbound link state routing with flooding reduction, lower levels are flooding their link-state information in the "northern" direction, so that each level obtains the full topology of levels south of it.
- Southbound distance vector routing, each upper node generated a default route to the "southern" direction.
- Link state is advertised one-hop southbound and then reflected one-hop northbound. This is when a node detects that default route encompasses prefixes for which one of the other nodes in its level has no possible next-hops in the level below, it has to disaggregate it to prevent black-holing or suboptimal routing through such nodes.
- Optional Zero Touch Provisioning (ZTP), only top tier nodes need to be configured.
- Packet formats are defined in Thrift [ROUT.29] models.

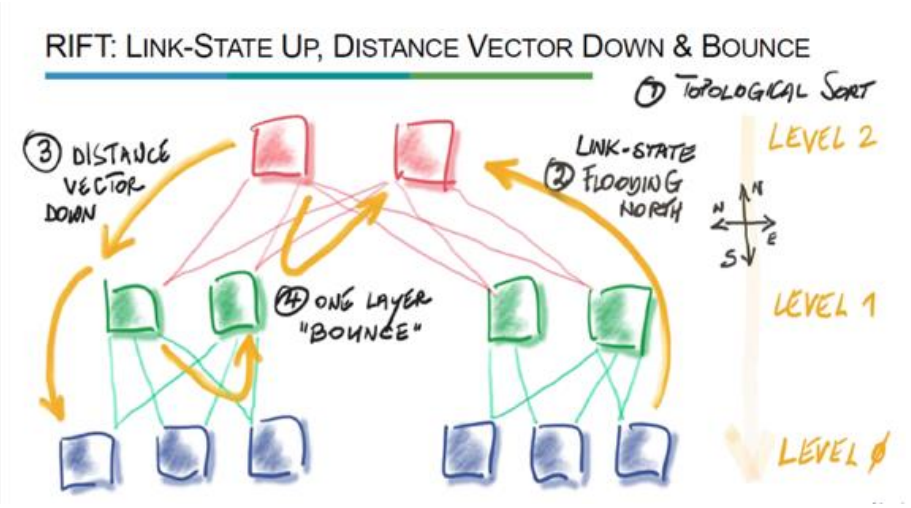


Figure 48- Illustration of RIFT: Routing in Fat Trees [ROUT.9]

- LSVR

The Link State Vector Routing (LSVR) working group [ROUT.31] at IETF is proposing a new solution which leverages BGP link-state distribution and the Shortest Path First (SPF) algorithm, and targets Massively Scaled Data Centers (MSDCs). The solution has the advantages of both BGP and SPF-based IGPs, including TCP based flow-control without periodic link-state refresh, thus provides a scalable solution in MSDCs where there are a high degree of Equal Cost Multi-Path (ECMPs). Like link state IGPs, the solution also supports fast convergence and Loop-Free Alternatives (LFAs).

- New BGP-LS-SPF SAFI for backward compatibility
- Nodes have complete view of topology
- Re-use BGP NLRI distribution
- BGP-LS encoding

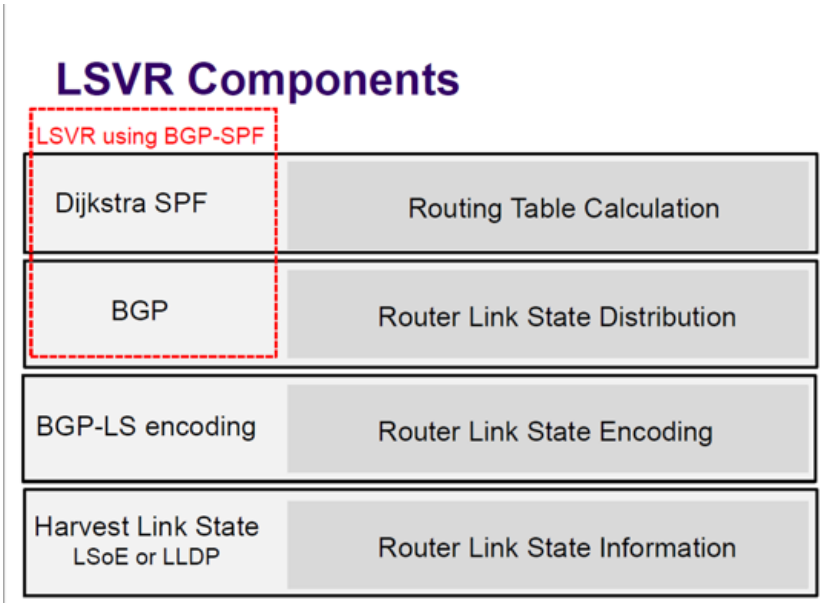


Figure 49- LSVR [ROUT.32]

- SCION

  The SCION (Scalability, Control, and Isolation on Next-Generation Networks) inter-domain network architecture has been designed to address security and scalability issues and provides an alternative to today's BGP. SCION combines a globally distributed public key infrastructure, a way to efficiently derive symmetric keys between any network entities, and the forwarding approach of packet-carried forwarding state. Instead of relying on inter-domain routing tables, the AS-level forwarding path is encoded in the header of the packet. Each router verifies a message authentication code with a symmetric cryptographic key before forwarding. A summary description of SCION can be found at [ROUT.33].

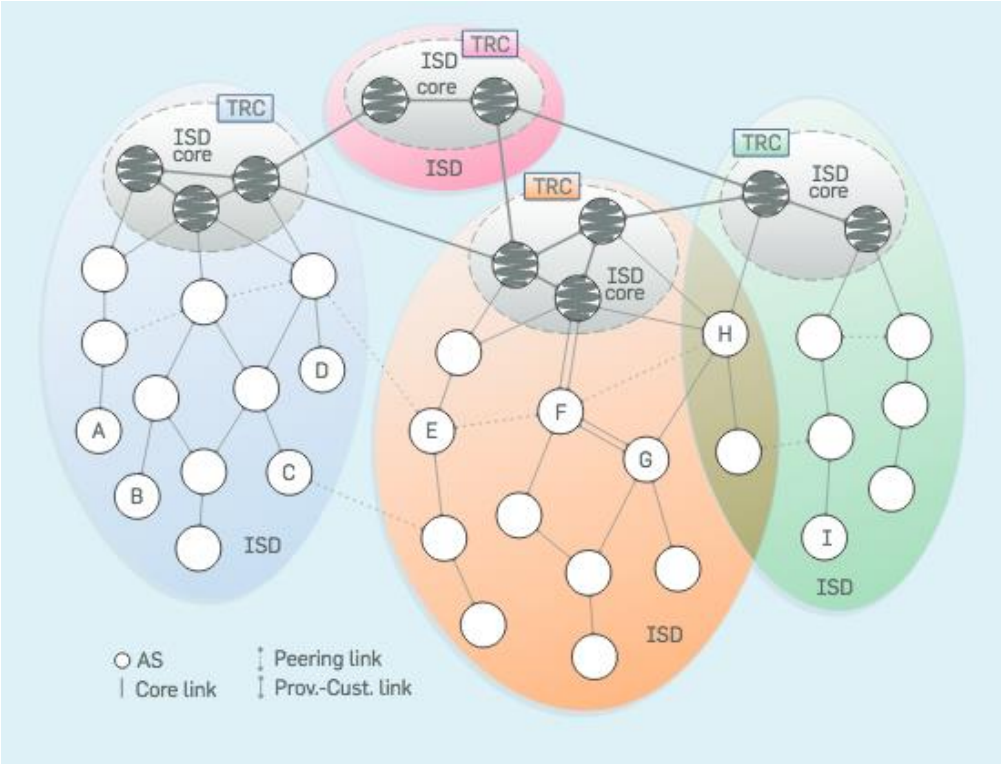


Figure 50- SCION Architecture Overview [ROUT.33]

A summary description of SCION can be found at [ROUT.33].

The SCION internet architecture provides a fundamentally clean-slate approach to multipath communication: at the control plane the routing system discovers a variety of AS-level path segments (which can also differ in the interface or links connecting neighboring ASes), which are globally disseminated through a path server infrastructure; at the data plane, cryptographically protected packet-carried state encodes the AS sequence and the AS-to-AS interfaces in the packet header.

End-hosts fetch viable path segments from the path server infrastructure, and construct the exact forwarding route themselves by combining those path segments. The architecture ensures that a variety of combinations among the path segments are feasible, while cryptographic protections prevent unauthorized combinations or path-segment alteration. The architecture further enables path validation, providing per-packet verifiable guarantees on the path traversed.

SCION’s intrinsic multipath communication provides a natural defense against distributed denial of service (DDoS) attacks. An attacker must congest all paths instead of only one, which increases the needed attack capacity and complicates the attack since access to all paths must be prevented. Further, an AS can choose not to publicly announce some of its path-segments at the path servers, but still share them with select communication partners “out of band”. The ability to use such “hidden” path segments as part of multipath communication guarantees the existence of a fall-back path that is not publicly known, and therefore cannot be clogged through a DDoS attack.

13 Security, Privacy and Trust

Given the broad scale of Security, Privacy and Trust, we need to properly scope these notions and to define them. First off, we are going to consider these notions mainly in the context of inter-domain network infrastructures -- as the challenges are much reduced in an intra-domain context, which is typically under single administrative control. We consider the security and trust of end-hosts and the privacy of data stored on end-hosts to be out of scope for this document. We do consider the security of network infrastructure devices, however, as their compromise can result in threats to network security. We will focus on network properties and not on individual services, unless the services are directly relevant to achieve the properties we seek.

We pursue security in terms of these network properties: A network is considered secure if it can achieve the desired properties even in presence of an active adversary. One prominent such property is availability, i.e., the control-, data-, management-, and configuration-planes should be protected such that an adversary cannot disrupt basic communication connectivity. Another important property is trust, which we understand here as the capability of network nodes to verify origin and content authenticity of messages passed through the network. Furthermore, a desirable, but hardly achievable property is privacy, treated here as the capability of nodes to communicate without outsiders identifying the parties of the communication.

In order to concretize the notions of security, privacy and trust, we state the goals of a secure inter-domain network infrastructure in Section 13.1. While pursuing these goals, a number of requirements has to be respected, which are listed in Section 13.2. Finally, Section 13.3 sketches possible pathways for achieving security and trust under the mentioned requirements.

13.1Goals

According to the [Sub-Group 1.1, Sub-Group 1.2], the design of security, privacy and trust of Network 2030 should contain the following features:

- **Improved trust model:** A new network trust model should be deployed to provide decentralized verifiability. Based on the new model, important network information, such as BGP, DNS and RPKI information can be verified in a more trustworthy way to prevent any single point of failure. The network trust model should also provide trust transparency, i.e., for any piece of information, a verifier should be able to identify all entities that have to be relied upon for the information to be trusted.
- **Efficient and scalable authentication mechanisms for AS and host-level information:** Such properties will prevent IP source address spoofing attacks, for instance. Such a service could enable a receiver to verify the origin of error packets.
- **Pseudonymous sender/receiver privacy:** Untrusted nodes in the network cannot identify the sender and/or receiver of communication without resorting to timing analysis (contrast with *perfect* sender/receiver privacy below). This property is typically achieved by identifier-translation services. Note that there exists an inherent tension between the goals of privacy and source accountability.
- **Availability in the presence of an active adversary:** Communication between two endpoints should be possible, as long as a functional and connected sequence of intermediate network devices and links exists. This is the foremost goal of network to provide utility to demanding use cases. A particular challenge is to ensure a Service-Level Objective (SLO) or Service-Level Agreement (SLA) even in adversarial contexts.
- **Transparency and control for forwarding paths:** Network paths in today's Internet lack transparency. In a first step, it would be useful to know as a sender which entities a packet traverses. In a second step, it would be useful for a receiver to achieve ingress path control. Finally, in a third

step, end-hosts could benefit from controlling the packet's forwarding path. These are important properties to prevent eavesdropping and man-in-the-middle attacks of intermediate entities, as well as to increase availability in case of maliciously congested paths that can be circumvented with path control. An important aspect of this property is path correctness: The sender should be able to verify path information and the receiver should be able to verify for each packet that the selected path was correctly followed. As a result, an off-path adversary should not be able to alter a packet's path.

- **Algorithm agility:** Cryptographic algorithms need to be replaced in case of breakthroughs in cryptanalysis or computation technology such as quantum computers. Thus, it is necessary that the network architecture and infrastructure are prepared to replace cryptographic mechanisms. A challenge is if algorithms are implemented in hardware, which requires a hardware replacement cycle to upgrade. Consequently, techniques need to be devised to retain secure operation through a potentially multi-year algorithm replacement cycle.
- **Class of security level:** Not all applications or processes need the same level of security. Security schemes typically require additional resources or time which may not be necessary nor available in some scenarios. A class of security level should be considered to support different requirements.

There are other network properties, which, albeit desirable, should not be provided by the network infrastructure itself, either because the properties can be achieved without network support or because the properties are too costly to achieve as basic network primitives. We thus consider the following goals to be out of scope:

- **Communication secrecy:** Achieve confidentiality for communicated data. This property is typically well understood and can be achieved with encryption between the end points, for instance using a VPN.
- **Perfect sender / receiver privacy, anonymous communication:** Untrusted nodes in the network cannot identify the sender and/or receiver of communication, even when performing timing analysis. Although sender and receiver identities can be concealed by name-translation services, perfect privacy can only be achieved by thwarting timing attacks, which requires an expensive traffic-mixing infrastructure.

13.2 Requirements and Challenges

The nature of inter-domain networks constrains the set of security solutions that are practically feasible. To achieve meaningful progress for the broad challenge of "security, privacy, and trust in networks", we provide a list of requirements that have to be respected by any security-improvement proposal:

- **Heterogeneous trust relationships:** Difficult to establish globally accepted trust roots. Allowing for choice among decentralized, diverse trust roots (sovereignty) is therefore important.
- **DoS and DDoS attacks at all levels (e.g., also against services, infrastructure, etc.):** The diversity of different types of (D)DoS attacks is very large, for instance algorithmic complexity attacks on the implementation, or resource exhaustion on a network link (bandwidth) or service (computation).
- **Difficulty of providing latency guarantees:** Due to complexity of inter-domain networks and interactions between high numbers of flows, latency guarantees are very challenging to achieve even in non-adversarial contexts. When considering an adversary, latency guarantees become exceedingly challenging.
- **Protocol complexity requires formal verification:** Modern distributed systems reach a scale that eludes people's mental capacities for considering all possible states and interactions, thus necessitating automated protocol verification techniques. Such formal verification achieves a high level of assurance. Protocol flaws can be avoided through formal verification tools, such as [Coq, ProVerif, Tamarin]. However, verification tools encounter scalability challenges with increasing protocol complexity.
- **Large network-technology diversity:** Ensuring security properties across ManyNets, a wide diversity of different network technologies, is a challenge. For instance, resource-constrained network environments may not provide sufficient resources to carry needed cryptographic information in each packet.
- **Software vulnerabilities throughout infrastructure and applications:** Although not directly connected to network security, the fact that some network infrastructure devices and end points will be under the control of an adversary need to be considered. Implementation security can be achieved through formal code verification, which unfortunately is still quite costly and does not scale well beyond tens of thousands of lines of code. Current state-of-the-art tools for code verification include [Dafny, Viper]. Examples for large-scale verification efforts include the seL4 secure microkernel, the project Everest verified HTTPS stack, or the VerifiedSCION project. API-level attacks can be prevented through the combination of protocol and implementation verification techniques.

In addition to the nature of inter-domain networks, the adversary model constrains possible security solutions. A general adversary model should consider the following types of attackers:

- **Nation-state adversary:** well-funded, large amount of trained personnel and infrastructure resources, can exploit vulnerabilities in devices, set up malicious entities / infrastructure, or control a large number of devices for DDoS attacks. Among main motivation are industrial espionage, critical infrastructure attacks at the network level, and preventing network availability in general.
- **Criminal organization:** significant resources, can control a smaller amount of infrastructure resources than the nation state adversary. Main motivation is to profit through contracted attack services, to a lesser extent espionage.
- **Independent hacker groups:** individuals or small political and ideological targets, smaller-scale attacks.

Ideally, even for nation-state adversaries, the security properties shall be achieved assuming existence of a network path that is not controlled by the adversary.

13.3 Design Alternatives

In this section, we present design proposals for achieving the goals laid out in Section 13.1, where each of the following subsections corresponds to a security goal. It is important to note that there exist dependencies between individual design proposals. For example, the decentralized trust model introduced in Section 0 enables the source-authentication architecture presented in Section 13.3.2.

13.3.1 Decentralized trust model

The currently existing public-key infrastructures, e.g. the DNSSEC PKI, the TLS PKI and the RPKI used in BGP, are designed based on a centralized system architecture or a centralized trust model. This kind of centralized architecture suffers from the problem of trust-anchor failure. In the centralized model, since descendants need to rely on some common ancestors or authorities as trust anchors, a central authority node has privilege over all the descendants. Central authorities can unilaterally perform malicious actions like revoking certificates, issuing fraudulent certificates or providing fake information. Since all these infrastructures are widely used across the world, malicious actions of central authorities may adversely affect the Internet. Trust anchor failures may happen for many reasons. A central authority may be hacked or compromised to perform malicious actions unintentionally. In other cases, an authority may not be fully neutral and perform malicious actions for economic gains or political reasons.

For Network 2030, a decentralized trust model should be provided. A first example is the SCION secure network architecture [8SEC.1]. In SCION, the Isolation Domain (ISD) comprises a group of autonomous systems (AS) and enables setting localized trust roots defined in a trust root configuration (TRC). The ISD can operate independently of any external network entity, and thus achieve sovereignty and address global heterogeneous trust relationships. The TRC of each ISD serves as the root of trust for the local control-plane PKI [8.2], which provides AS-level certificates. Thanks to the structure of SCION's control-plane PKI, trust transparency is achieved.

An alternative design is shown in **Error! Reference source not found.**, its DII architecture consists of t hree layers. The underlying layer is the distributed ledger layer, providing decentralized trust foundation for DII [8.3]. The intermediate layer, called name space management layer, fulfills the management of Internet core resources (such as IP addresses, AS numbers and domain names) in a decentralized and trusted manner. Based on the distributed ledger technology, the intermediate layer can provide trustworthy resources ownership for resource owners. Furthermore, based on resource ownership, the intermediate layer can further provide trustworthy mapping information between different resources. The mapping information can be used to fulfill the fundamental functions of BGP, DNS and PKI. The top layer is an

open application layer which can support more trustworthy Internet applications with the trustworthiness provided by lower layers.

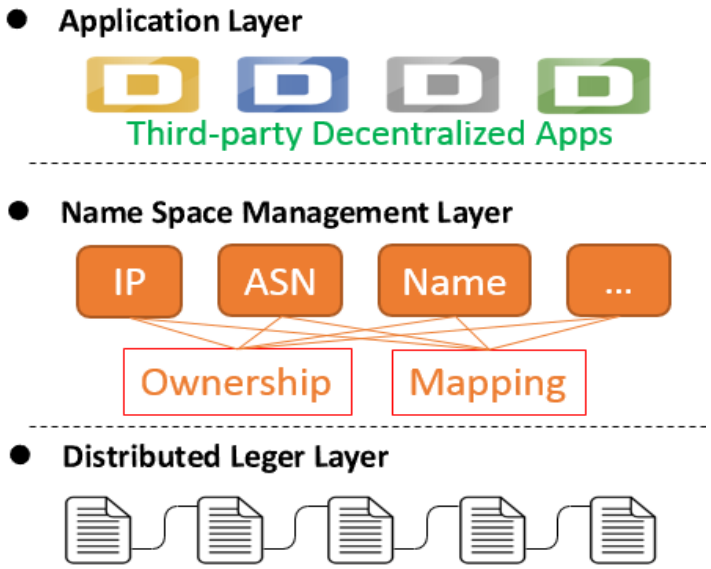


Figure 51- DII Architecture Design

13.3.2 Efficient authentication mechanisms for AS and host-level information / Pseudonymous sender-receiver privacy

In this section, we present an approach (NAIS, Network Architecture with Inherent Security features [SEC.4]) for authenticating packets in an inter-domain network. The goal of NAIS, which is structurally analogous to the APNA system [SEC.5], is to provide source authentication while preserving privacy of the communicating parties. In order to reconcile these conflicting objectives, domain operators act as privacy brokers for their internal hosts. **Error! Reference source not found.** illustrates the basic idea of N AIS: A host with ID HID obtains an EID (ephemeral/encrypted ID) from the local Identity Manager (IDM), as well as an ELoc (ephemeral/encrypted locator) from a local DHCP server. When sending a packet, the host then uses the ELoc as source information instead of its real location. In the source domain, EID and ELoc are checked on their validity by both internal routers and border routers, both of which do not learn the real identity of the host. For inter-domain traffic, border routers obfuscate the ELoc in the packet header and add a verifiable domain tag (ASID) to attest that the packet originated from the local AS.

This tag contains a MAC, based on a symmetric key that the source AS shares with the destination AS. By building on the decentralized PKI proposed in the preceding section, such a symmetric key can be negotiated, which allows the destination AS to verify the ASID tag in packets. In case of a misbehaving flow, the destination AS can then contact the Auditing Agent (AA) in the source AS, notifying it that the host with a certain ELoc needs to be blocked. As the AA is trusted, it can derive the true HID from the ephemeral information and instruct the local routers to block the corresponding traffic. Using this mechanism, NAIS prevents IP source spoofing attacks and DDoS attacks (as long as the source AS is trusted). The short-term validity of ephemeral information reduces the feasibility of association analysis, ensuring a relatively high degree of privacy for users. However, we note that packet-level timing attacks would still be possible in this system, which limits the privacy of users.

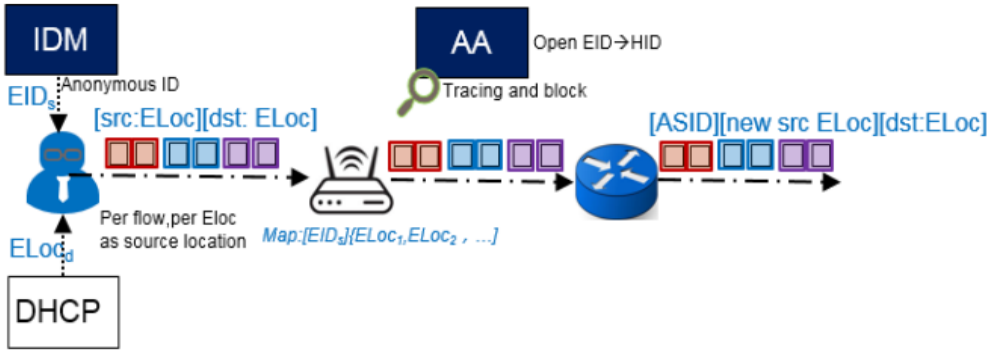


Figure 52- Dynamic and privacy-preserving auditable ID/Locator

In some scenarios, the NAIS approach to source authentication has to be adapted for the sake of efficiency. For instance, consider a host H in an AS A_1 that wants to authenticate an error message from a router R in a remote AS A_2. With the standard NAIS approach, the host H would need to contact its local AA in AS A_1, which could authenticate the source of the error-message packet. For the sake of efficiency, this authentication would be performed on the basis of a symmetric key that the local AS A_1 shares with the remote AS A_2. However, since this key must not be shared with the host H that requests the authentication, involvement of the local AA would be needed for authentication of every error packet, making authentication prohibitively expensive in repeated application.

This problem can be addressed by the DRKey (dynamically recreatable keys) system of SCION [8.6], which could be employed as follows. The egress border router of the source AS could compute the authentication tag of the packet on the basis of a dynamically recreatable key specific to the destination *host H*, instead of a static key specific to the destination *AS* A_1. More formally, the symmetric key used in MAC computation at the source egress would be $K(A_1{:}ELoc_H, A_2)$ instead of $K(A_1, A_2)$. The source egress border router could derive $K(A_1{:}ELoc_H, A_2)$ by means of a HMAC computation with key $K(A_1, A_2)$ and argument $ELoc_H$. Standard hardware allows such a derivation to be highly efficient, even more efficient than a memory lookup for stored keys. The AA in the destination AS could perform the same derivation and provide $K(A_1{:}\ ELoc_H, A_2)$ to host H. As a result, host H could verify all packets from AS A_1 on its own after only one request to its local AA, which is necessary to learn $K(A_1{:}ELoc_H, A_2)$.

Using this lightweight and privacy-respecting approach to source authentication, Network 2030 can inhibit IP spoofing and attacks that make use of IP spoofing, such as session hijacking, man-in-the-middle attacks, and DDoS attacks. By verifying the packet origin at multiple places in the network (**Figure 53**), the network performs *minimum trust-based authentication*: As soon as one verifier cannot verify the packet origin, the packet is dropped. In the case of cross-domain transmission, the internal ID verifiers, the border router of the source domain and the border router of the destination domain will verify the outgoing traffic. Therefore, it is not assumed that the ID verifiers are completely trusted. Moreover, such a multiple-verification design stops malicious traffic early in the network and prevents malicious traffic from converging on the victim host, thereby limiting the effectiveness of DDoS attacks. However, DDoS attacks are still possible if the source domain is malicious, e.g., if the source domain does not restrict flows that misbehave despite blocking requests from the destination domain. Even if the destination domain identifies the source domain as malicious, the border router of the destination domain as well as the paths leading to the destination domain could be overpowered by a sufficiently powerful malicious source domain. If a DDoS attack is carried out by an attacker with AS-level capabilities, the QoS systems described in the next section are required.

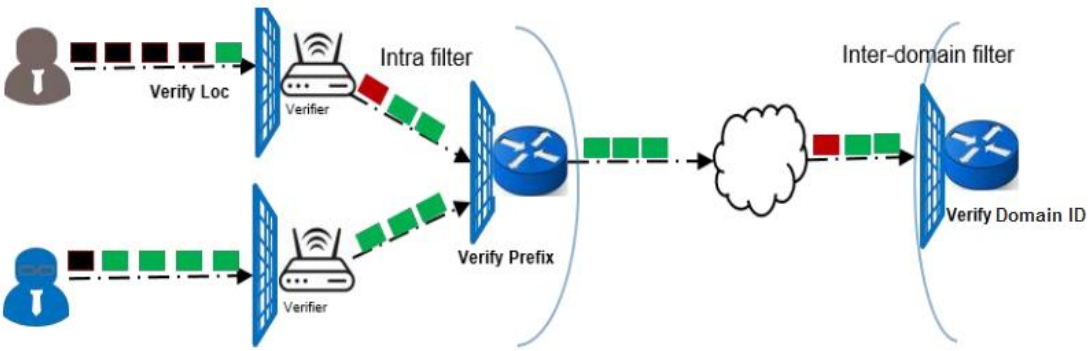


Figure 53-: Minimum trust-based authenticity verification

13.3.3 Availability in presence of an active adversary

DDoS attacks are still a stubborn problem that undermines network availability. In 2018, DDoS attack traffic has exceeded 1.7Tbps. As more heterogeneous IoT devices are deployed across the Internet, DDoS attack threats will continue to intensify and break the existing firewall-based security defense baseline. 5G network technology will support millions of connections per square kilometer, so DDoS attack traffic from the same administrative domain should not be underestimated.

As explained in the previous section, multi-level verification on the basis of NAIS can prevent DDoS attacks in some cases. However, if the attacker has AS-level capabilities, this line of defense fails, as a malicious source domain can continue to overload targets along a certain path while ignoring the shut-off requests from the destination domain. For such attacks, quality-of-service (QoS) systems based on bandwidth reservation are an effective mitigation tool.

The rationale of bandwidth-reservation systems is as follows. In return for a payment, end-hosts obtain a share of the available bandwidth along a certain path. The reserved bandwidth amount is the assured minimum amount of bandwidth usable in any case, i.e., even in case of a link overload along a path. In case of a link overload, flows on the link without a reservation might be dropped, while flows with a reservation can continue using the link to the extent of their reservation. The bandwidth not used by flows with reservations is available to flows without reservations on a best-effort basis. With a bandwidth-reservation system in place, predictable quality of service can thus be ensured even in the presence of AS-level attackers.

In order to obtain a reservation, an end-host would need to send a reservation request along the desired path, where the request would contain the desired amount of guaranteed bandwidth. When passing the request in the initial direction, every AS on the path incorporates into the packet the amount that the AS is ready to allocate for the reservation. After reflection at the destination, the ASes along the path could then allocate the actually available bandwidth, given by the minimum amount of bandwidth that has been appended to the reservation request. **Figure 54** Error! Reference source not found.Error! Reference source no t found. illustrates the reservation process. Developing a scalable, fair and efficient method of bandwidth allocation is a subject of ongoing research.

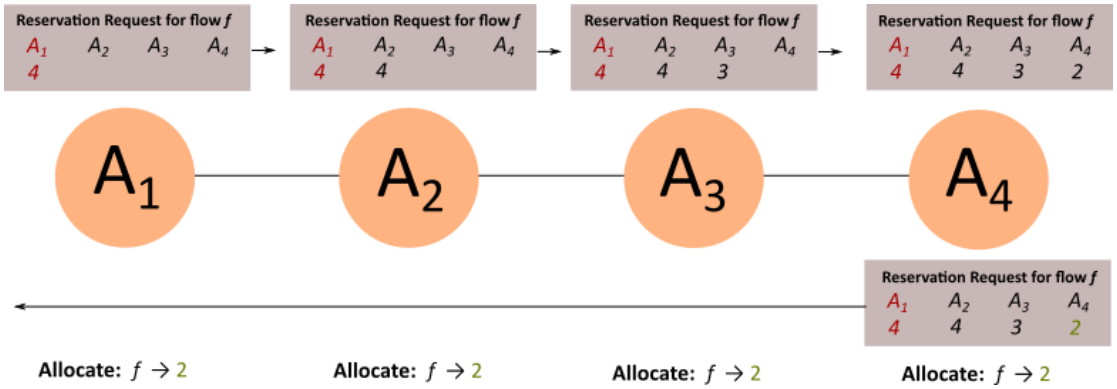


Figure 54- Distributed management of reservation requests in bandwidth-reservation architectures

When passing back the reservation request, every AS also inserts a reservation tag into the packet, which cryptographically protects the AS-specific reservation information. This reservation tag is a MAC, based on a local secret only known to the AS. An end-host with a reservation must include all the reservation tags for a path into its packets. When checking packets that include a reservation tag, each AS can efficiently verify that a flow indeed corresponds to a reservation, without keeping reservation state on the border routers.

13.3.4 Transparency and control for forwarding paths

An exciting development over the past decide are path-aware network (PAN) architectures, where senders embed the network path into the packet header. This seemingly simple concept results in exciting security opportunities for Network 2030. Packet-level path information enables delivery as long as the path is functional, independent of actions by the routing protocol. Path information also enable predictability of which ASes need to be relied upon for the packet to arrive at the destination. Given topological path information, the reliance on any single AS can be minimized by using multipath transmissions over maximally disjoint paths. Moreover, topological path information allows to exclude some routes altogether, e.g., for the purpose of surveillance resistance. Stable paths are also a necessary precondition for future QoS mechanisms that are based on bandwidth reservation along paths (cf. Section 10.3.3). Even without QoS systems in place, transparency and control over forwarding paths provide protection against DDoS attacks, as path control allows the circumvention of maliciously congested paths (given that alternative paths exist).

However, path awareness requires dissemination of path information, which is confronted with the following three challenges. First, path information must be disseminated in an authenticated fashion such that the information can be verified. Second, path information must be disseminated in a scalable fashion, i.e., the dissemination complexity in terms of messages should not become overwhelming in large topologies. Third, path information, in particular dynamic path properties such as load on the path, should be disseminated in a timely fashion in order to be useful.

In order to solve these challenges, the key idea in the SCION network architecture is to use a form of network partition, i.e., to split the network into *Isolation Domains (ISD)*, each containing multiple ASes (**Figure 55**). A subset of ASes in each ISD form the ISD core, which both initiates intra-ISD path discovery and provide inter-ISD connectivity. For intra-ISD path discovery, an ISD-core AS sends a beacon to each of its customer ASes, where the beacon contains information about the link to the respective customer AS. In turn, each customer AS forwards the beacon to its own customer ASes after updating the beacon with the necessary link information, and so on. The same path-segment construction process takes place between core ASes of different ISDs. The resulting path segments can be combined to connect any AS to

any other AS. For this purpose, the core ASes maintain a destination-based database of active path segments and respond to path-segment queries of other ASes.

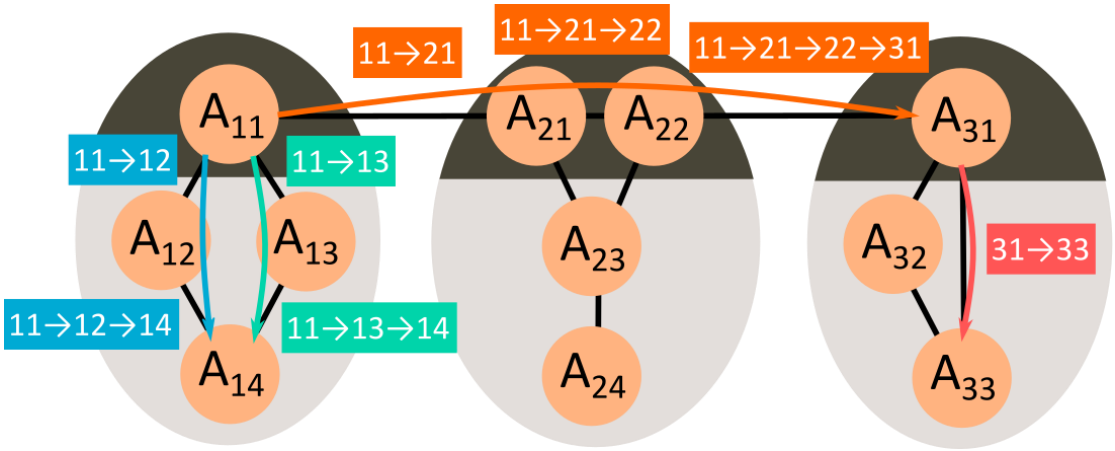


Figure 55- Path-information dissemination across Isolation Domains

The segmentation of paths allows the path-discovery process to remain scalable while preserving universal connectivity. In comparison to pure source routing, segmentation is much more scalable while only marginally reducing the space of possible paths, as business-logic constraints on possible paths are practically identical with the constraints enforced during segmentation. Since the number of individual path-dissemination messages is reduced, their frequency can be increased, leading to a more up-to-date view of the network. Moreover, isolation is a security feature, as intra-ISD forwarding is completely independent of the less trusted exterior ISD network.

In order to protect the integrity of constructed path segments, the beacon-forwarding AS always has to include the AS to which the beacon is forwarded, as well as sign all the information added to the beacon (similar to BGPsec). In order to guarantee that a packet in fact follows the path selected by its sender, every packet carries a short representation of the path in its header which is cryptographically linked to the packet payload. Such packet-carried forwarding state allows any AS on the path to verify that the sender intended to send the packet through the AS (as well as the preceding AS from which the packet was received). Since forwarding misbehavior can be detected and deterred using this technique, the end-hosts gain control over the forwarding paths that their packets follow.

13.3.5 Algorithm agility

Algorithm agility is a property that allows to easily migrate from one algorithm to another one. It is especially important in the context of cryptographic algorithms, which become weaker over time. Since it is not possible to predict advances in cryptanalysis techniques, every future-proof architecture that employs cryptographic algorithms should provide a mechanism for algorithm agility.

In particular, achieving algorithm agility is a challenge if the exchangeable cryptographic algorithm has to be harmonized network-wide. In the following, we point out the elements of the proposed security architecture for Network 2030 where cryptographic algorithms are needed, and explain how to provide algorithm agility in these settings:

- **AS tag in NAIS source authentication (cf. Section 10.3.2):** When a packet leaves its source domain, the egress border router adds an AS-specific MAC to the packet, computed with a secret shared with the destination AS or the destination host. Clearly, the used algorithm for MAC computation can be negotiated between the communicating parties beforehand, providing flexibility in choice of the algorithm.

- **Computation of reservation tags in QoS system (cf. Section 10.3.3):** In the reservation process, the authenticity of AS-specific reservation information is protected by a MAC, resulting in a reservation tag. Since this MAC is only intended for the AS itself to verify, the MAC algorithm can be chosen at the discretion of the respective AS, without any coordination needed.
- **Signatures for path information (cf. Section 10.3.4):** In the path-discovery process, the path-segment construction beacons are extended by ASes with path information, which needs to be protected with a signature in order to be universally verifiable. In order to obtain algorithm agility for the signature algorithm, we envision that an AS can protect its added information by multiple signatures using different algorithms, while always explicitly naming the used signing algorithm. A consumer of created path segments can thus always check whether a trusted signature algorithm was used in the creation of the path segment. Algorithm diversity may also give rise to varying security properties across path segments in a transparent manner, enabling end-hosts to take account of the desired security level in their path selection.

13.3.6 Class of security level

Although security is desirable for almost any use case in an inter-domain network, security often comes at the price of additional processing, latency or complexity, reducing the efficiency of communication. For some use cases, it may thus be desirable to trade security for efficiency. An end-host should thus be able to employ security functions depending on the desired security properties. The proposed security architecture for Network 2030 allows an end-host to adapt its guarantees to its demand for security in manifold ways:

- **Privacy and source authentication and with NAIS (cf. Section 10.3.2):** In NAIS, achieving sender privacy requires address translation process by the AS. If an end-host is not interested in privacy, it must use its real IP instead of an ELoc as source IP and signal in the packet that no address translation is needed (alternatively, bypassing address translation could be the default option). Source authentication requires a MAC computation by the home-AS border router, which could be instructed to not perform this origin authentication. However, it depends on the ingress policy of the destination AS whether such non-authenticated traffic would be accepted.
- **Bandwidth reservation for a QoS system (cf. Section 10.3.3):** By design, bandwidth reservation is an on-demand service. An end-host can purchase a bandwidth reservation for critical communication or rely upon best-effort transmission for less critical communication. By adapting the reservation amount, an end-host can obtain the optimal degree of insurance against link overload.
- **Path awareness (cf. Section 10.3.4):** Having path awareness allows an end-host to strike the optimal balance between security and performance in a multitude of ways. For example, an end-host can leverage path information to balance the degree of multipath transmissions with the overhead of managing multiple connections. Moreover, an end-host can choose paths according to performance properties (bandwidth, latency, loss, etc.) or according to security properties (location, confidence in path-information authenticity, disjointness, etc.).

13.3.7 New roles and features

In this section, we aim at listing the new devices, services, and processes that are needed in the security architecture proposed in Section 13.3.

13.3.7.1 NAIS for source authentication and privacy

In Section 13.3.2, we presented NAIS, a network architecture that enables source authentication in an inter-

domain context while preserving sender and receiver privacy. In summary, domain operators act as privacy brokers for their internal nodes, forwarding packets with a pseudonymous address as source IP but certifying that the packet originated from within it. Internally, the AS takes precautions against spoofing. Given a misbehaving flow, the destination domain can direct a so-called shut-off request to the auditing agent of the source domain such that the malicious traffic is stopped early. **Figure 56** presents the NAIS architecture in detail, with all the new devices and services needed:

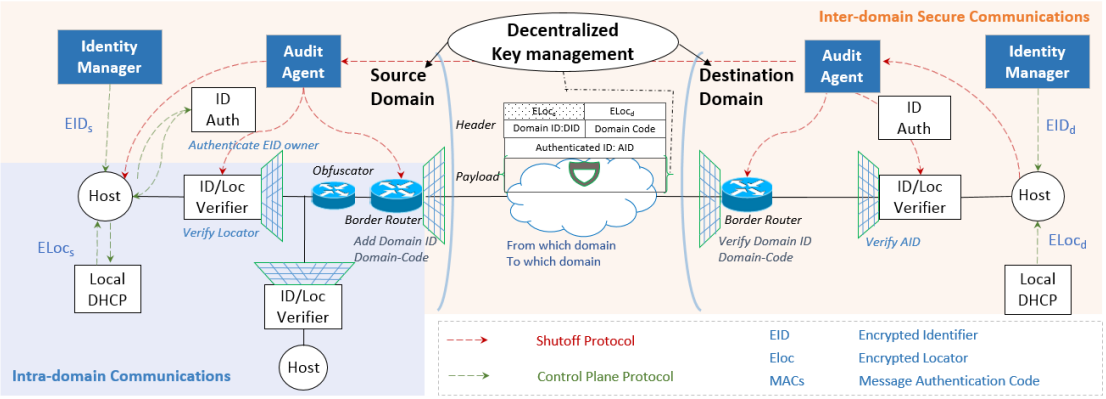


Figure 56- Network Architecture with Intrinsic Security

- The **Identity Manager** is responsible for managing the identities of hosts within a domain and distributing a permanent *Host Identifier (HID)* and an *anonymous ephemeral and encrypted identifier (EID)* and its credentials for each host.
- The **ID Authenticator** authenticates the EID owner, checking whether a certain host possesses the credentials for a certain EID. If yes, the host obtains an authentication tag that will allow it to obtain an ELoc from the Local DHCP server and pass the ID/Loc Verifier.
- The **ID/Loc Verifier** is a router with authenticity verification function that verifies the authenticity of the sender and filters out spurious or malicious packets.
- The **Obfuscator** takes charge of translating the internal ELoc to an external ELoc which can be frequently changed to impede association analysis.
- The **Local DHCP server** manages and distributes ephemeral and encrypted Locators (ELoc) to hosts within a domain.
- The **source domain border router** also verifies the authenticity of the source before forwarding packets to the Internet, and adds a *domain ID (DID)* and a *domain-code* as a verifiable domain tag. When the packet arrives at the destination domain, the corresponding border router can filter out the fake source packet by verifying the authenticity of the source domain ID.
- The **Audit Agent** is responsible for tracking and auditing illegal traffic.

13.3.7.2 Bandwidth-reservation system for inter-domain QoS

For bandwidth-reservation systems such as the system proposed in Section 7.3.4, every AS requires a reservation accounting server that manages the reservation requests arriving at the border routers, as well as keep track of available bandwidth that can be reserved. The border routers need to be extended with MAC computation functionality such that the data-plane processing can verify the reservation tag in packets.

13.3.7.3 Path-aware network architecture

In order to enrich Network 2030 with inter-domain path awareness, additional services are needed. For instance, in the SCION architecture every AS deploys the following two additional services:

- **Beacon service:** Required for managing the path-segment construction beacons. The beacon service adds the relevant information to beacons and forwards the beacons to downstream ASes according to the domain's policy.
- **Path service:** Required for enabling lookups of paths for a given destination. The path servers cache path segments for the network topology, providing end-hosts with the necessary information to reach destinations. In case there are no cached path segments for a given destination, the path service of a domain requests corresponding path segments from another path service, usually from an ISD core path service.

In order to grant path control to end-hosts, border routers must be extended such that the data-plane processing can check the path representation in the packet header. In particular, the border routers should be able to verify that the packet in fact follows the intended path and that this intended path is valid.

14 QoS

14.1 Introduction

This section abstracts the networking infrastructure for Internet and private networks towards the conceptual building blocks described here. These will be used as references in the document for the feasible/required functionalities.

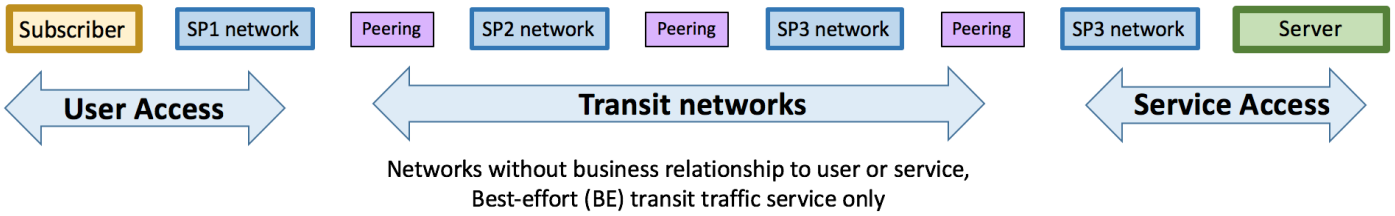


Figure 57- Traditional Internet service model: worldwide end-to-end network paths with transit

QoS for Network 2030 as discussed in this document is based on leveraging the evolution of the reality of the Internet architecture. In its original form, as shown in the picture above, the Internet service is concerned with traffic between Subscribers and Servers that are interconnected by so-called end-to-end network layer transit paths. In these paths, traffic is passed through so-called networks without business relationship to subscriber or server. This is one of the core reasons why in the traditional Internet service model, only "best-effort" (BE) traffic is supported.

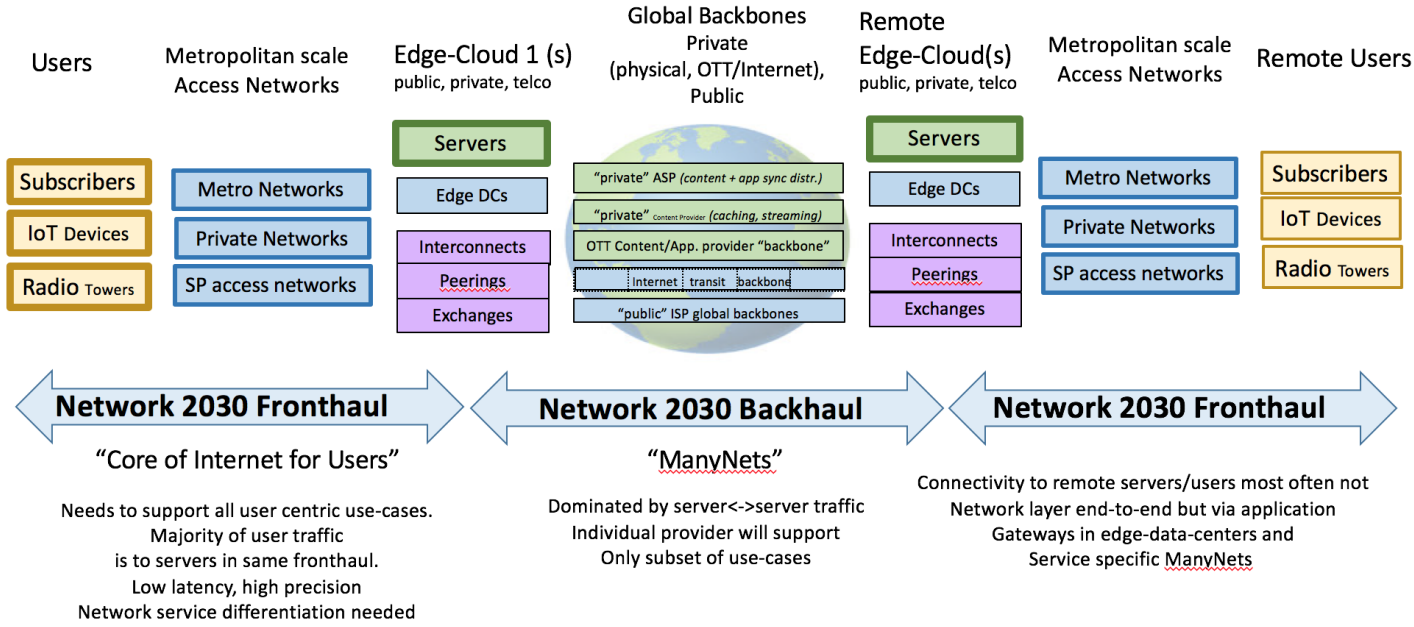


Figure 58- Expected Evolution of Network2030 Architecture

Network 2030 QoS evolution is primarily important for the Subscriber edge where latency and services better than best effort will be required by Network 2030 applications. This will be here "Network2030 fronthaul" and reaches up to the Edge Compute/Data-Centers. A metropolitan region is a typical instance of a fronthaul.

Focussing on this part of the network also allows to reduce the business and architectural complexity of providing differentiated QoS offering because it can eliminate pure-transit network issues.

Backhaul networks will have specific QoS requirements/opportunities, but to the extent that these go beyond a subset of those QoS functions required in the fronthaul, these will separately be considered for such specific type of backhaul networks.

.

14.2 Fronthaul and Backhaul

Physical network infrastructure in 2030 can roughly be divided into a "fronthaul" and a "backhaul". Fronthaul/Backhaul are interconnected by Edge-Data-Centers, Exchanges/Interconnects and private peerings. This is called the fronthaul/backhaul edge. In the case of a classical Internet Service Provider, the fronthaul/backhaul edge could be the Central Office (CO) as long as these would be sufficiently close to the network subscribers to permit latency constrained services. FOr example, if they are co-located in a metropolitan area with subscribers.

The "fronthaul" of the network infrastructure consists of metropolitan size physical networks owned/operated by classical Internet/Network-Services providers, Application Service Providers (ASP e.g.: FAANG), cities and other public operators and other private networks (such as large manufacturers, transportation companies and the like). These networks physically connect a set of users and/or (IoT) devices amongst each other via wired/wireless access and towards the fronthaul/backhaul edge.

The "backhaul" of the network infrastructure consists both of the multi-AS hop "classical Internet" as well as a variety of private networks owned by variety of institutions, Network Service Providers, Application Service Providers, Public Operators and more specialized network operators.

.

14.3 QoS in the fronthaul

The majority of application traffic flows that do involve subscriber will stay within the fronthaul because it is the part of the network connecting to subscriber. This includes for example consumer entertainment traffic from Edge-DC to consumers, and where it is desirable for lower latency also directly between subscribers, for example with interactive Virtual Reality (VR), Augmented Reality (AR) or holography between subscribers.

New classes of applications such as Car2X communications and still very much evolving Machine 2 Machine communications in industrial solution or other command and control within the city will evolve with their own traffic flow characteristics which may be more or less centered in the Edge-DC than current widely deployed type of applications.

While content/traffic for applications may and will ultimately extend far beyond a single metropolitan area, it should be expected that it will not flow end-to-end at the network layer, but instead it will be segmented at the application level at Edge-DC. This trend is already very strong in today’s evolution of applications via distributed cloud based application instances. One of the key reasons is that more and more of the backhaul network infrastructures are in effect privately owned by ASP, and access and resource management to their backhaul is managed and only possible to applications running on those ASPs Edge-DC.

Included in these Edge-DC applications are also virtual overlay network services that do link and interconnect network layer access in the fronthaul with backhaul tunneling/transport of network layer traffic across private backhauls. Today this is most often part of solutions called Software Defined Wide Area Networks (SD-WAN). Likewise, 4G/5G core networks can be considered to be such intra-internet-fronthaul overlay applications consisting of 4G/5G user and control plane typically implemented in VMs running on Edge-DC systems and radio towers acting as another type of subscribers to the internet fronthaul.'

14.3.1 Benefits

The key benefits and simplifications of this expected evolution of network services to QoS are as follows:

14.3.1.1 Simplified QoS on paths across the fronthaul

Within the fronthaul, the physical (speed of light) caused latency is low enough to allow traffic flows between eny two points with very low RTT latency, for example 7 msec including switching latency in equipment. This allows support for all the foreseeable applications from FGNET 2030 SubG1:

Within the fronthaul, the number of operators involved in end-to-end paths will in most cases be limited to one provider for each endpoint of a network layer traffic flow, directly connected only via exchanges/peerings - whether an endpoint is a server in an Edge-DC, a wired/wireless user or (IoT) device. This is an important shift and simplification for QoS from today's traditional Internet paths, where traffic typically passes not only through those two "endpoint access providers", but through one or more additional "transit service providers" without any explicit business relationship to either of the endpoints.

To a large extent, the lack of support for better than best-effort QoS in the Internet is caused by the inability to develop working business and technical solutions to support such QoS across such multi-AS (Autonomous Systems) paths. In future network 2030 fronthaul, the simplification of these paths should enable the easier design of appropriate technical and business models to support the variety of QoS services desired for example by FGNET 2030 SubG 1 and SubG 2 results..

14.3.1.2 Flat network QoS design in fronthaul ("hop-by-hop PE")

For the purpose of this document, we consider that fronthaul networks should support the required per-hop functions on every hop. This is opposed to current standard Provider Core (P) vs. Provider Edge (PE) designs where QoS and other functions are hierarchically organized, whereas the PE nodes and external out-of-band systems take on the responsibility for QoS and resource management is done such that no QoS service "impacting" congestion/contention can happen on P nodes. This is done to easier scale at cost P nodes.

"Impacting" in the previous chapter does not mean that there cannot be any congestion/contention. For example, best effort traffic may still suffer on P nodes under higher loads of competing guaranteed bandwidth services, but there are for example no expectations for per guaranteed service latency management on P nodes.

The reasons for not expecting P/PE differentiation in the fronthaul is as follows:

1. Fronthaul networks should be able to support arbitrary, cost optimized topologies. Extrapolating from the past, this means that it could be complex topologies of subtended rings, which are the lowest cost captial expenditure (CAPEX) redundant topologies based on opportunistically available fiber trails. In these type of topologies, the probability for nodes having to be PE nodes is quite high and the benefit of optimizing the architecture to support reduced functionality P node modes may therefore not be significant for the additional system complexity that P-node support may introduce (depending on service) on PE nodes and the backend system.

2. P/PE distinction is an optimization that evolved at least 10 years after the required services where understood and deployed in flat topologies. As of today, mechanisms to support P-node equivalents of all future QoS services discusses are still evolving research topics and may hence may take longer to become available

14.4 QoS for the backhaul

Many backhaul networks will be built around the needs of specific use-cases only, so they will not be necessarily general purpose. Many of latency and resilience related service aspects will differ widely based on the use cases against which the backhaul network is design. Backhaul networks may even have even more complex requirements such as those of Low earth ... geostationary Satellite Networks, or network using on-demand capacity.

In result of these considerations, this section does not address specific backhaul QoS considerations. Instead, backhauls could adopt a subset of the QoS functions derived from the fronthaul considerations described here. Additional QoS functions specific to individual type of backhauls is better addressed in sections specific to those type of backhauls.

Note that backhaul networks may reach all the way to subscribers, such as planned LEO satellite networks with direct subscriber terminal. How such "direct-to-subscriber" backhaul networks integrate into the geographic fronthaul network of the region where the subscriber is located is subject to the QoS design of these specific backhaul networks.

14.5 New QoS services

14.5.1 Elastic, Experience Quality based resource management

The evolution of widely adopted audio and video solutions in the last 30 years has shown that media can be made elastic, e.g.: adjust to changes in available bandwidth. For RTP real-time communications, this reaches as far back as [QoS.5] from 1996. In a simple model, each media flow may have a minimum acceptable bandwidth (resulting in minimum acceptable experience quality) and a maximum desirable bandwidth (and resulting best experience quality). This is not only true for today’s media, but can safely be assumed to be true for at least part of future media such as holography.

As of today, there is no standardized model how these expectations should map to the allocation of network resources. When today flows compete through congestion control in the Internet, all flows are expected to roughly utilize the same amount of bandwidth. Under peak utilization, video streams with the lowest bandwidth for the best quality experience, such as small (tablet displays) will get the best quality, while the most expensive display devices (requiring higher bandwidth for the same experience quality) suffer most. Worse yet, traffic flows with arbitrary bandwidth requirements such as downloads will consume random, high amount of bandwidth, reducing the quality experience for all, more throughput critical applications.

Multimedia applications [QoS.8, QoS.9] were, early on, inherently multi-user and often operate in an environment where various participants are located on systems and communication links with different capacities and resource capabilities. Therefore, mechanisms were proposed that ensure appropriate quality media for different users. In order to achieve this, QoS filters were proposed as a way to adapt QoS to the user-specified level by changing the structure of a media stream in a well-defined way [8]. These filters are located along the data path (in contrast to adaptation that happens at the server side as is the case in DASH). Another advantage is that thereby one-to-many communication can also be supported. Using QoS Filtering in conjunction with other QoS provision allows for an integrated and optimised quality of experience (QoE) for individual users while optimising communication and system resources [9].

For network 2030, it is important to investigate better support for elastic resource management. While there have been early architecture proposals for dynamic QoS at a comprehensive architecture level, as far back as the 1990s e.g [7], this has not architecturally proliferated into current networks. Nevertheless, core mechanisms such as per-flow weighted congestion control schemes (e.g. NADA [6]) or congestion based bandwidth reservation adjustments (RSVP Multi-TSPEC [draft-ietf-tsvwg-intserv-multiple-tspec]) are recommended starting points at the lowest levels.

The main challenge are appropriate policy frameworks where experience quality and not only absolute bandwidth become accepted factors in resource allocation, especially under congestion/contention for resources.

14.5.2 Lightweight, scalable in-network resource guarantees

The more complex the network, the more complex resource reservation for bandwidth and even more so latency. At least with existing technologies.

Off-path reservations as described above suffers the problem of correctness in the face of complex dynamic path selection. SDN coupling has recently attempted to overcome this issue, but this results in very complex and fragile, tightly coupled systems. Nevertheless, this is the only currently feasible option in the absence of innovation for on-path resource management. It is therefore important for network 2030 to consider such innovation direction.

On-path bandwidth reservations such as via the RSVP protocol suffer the problem of scalability through per-flow control-plane state operations, and the 2000th decade successor to RSVP (NSIS) made the overhead of these control plane operations even worse through even more complexity.

Whereas forwarding plane performances grew by factors of 10,000 or more in the last two decades, the performance of control plane barely rose a factor 10 or 100 in the same time, so on-path resource reservation via traditional approaches such as RSVP, NSIS or similar evolving protocols in IEEE can only be adopted by investing into significantly faster control plane performance.

An even better solution is to design new, on-path resource reservation protocols that are lightweight enough to be processed not by the control plane but the actual (hardware accelerated) forwarding plane in 2030 network devices. Prototypes of such approaches for example with TCP exist and are documented, for example draft-han-6man-in-band-signaling-for-transport-qos.

Any form of reservations of bandwidth resources for network 2030 should support the handling of not only fixed reservations but also those of elastic media as described in the previous sub-section, by combining for example the mentioned approaches.

Whereas bandwidth reservations 'only' require accounting of per-hop/per-flow allocated bandwidth, guarantee of maximum end-to-end latency does require both bandwidth reservations AND per-hop per-flow state with today's widely accepted mechanism such as in IETF IntServ Guaranteed Services, TSN or currently envisioned DetNet mechanisms. Note that per-path aggregation of flows is possible to increase scalability.

This per-flow state whose complexity may range from a per-flow shaper to per-flow interleaved regulator support is likely infeasible to scale even to the size and scale of flows required in metropolitan aggregation networks where latency control can be critical with future network 2030 applications.

Solutions to provide better aggregated per-hop traffic shaping are being researched and promising. An example of this is cyclic queuing for IP networks as described in [draft-qiang-detnet-large-scale-detnet]. This too has been shown combined with the aforementioned in-band signalling to provide both bandwidth and latency guarantees, both bandwidth and latency guarantees.

14.5.3 Fine grained, path aware latency management

The previous sections summarized recommend directions for QoS architecture evolution int 2030 networks for the gaps for which research has already been done for a longer time:

1. Per-flow differentiated, non-reserved but congestion controlled bandwidth management, for example by supporting differentiated (weighted) bandwidths per flow.
2. Simplifying and scaling bandwidth admission control, by moving it to the high-performant/scalable forwarding plane.
3. Scaling guaranteed maximum (end-to-end) latency through forwarding plane mechanisms with less than per-flow complexity.

What these points do not cover is the differentiation of traffic in the network in a more fine-grained fashion by its latency requirements.

These latency aspects are investigated in the Network2030 SubG2 output document by considering the requirements of the FGNET SubG1 application requirements, especially including the requirements for in-time vs. on-time latency management as part of high-precision-communications and coordinated communications:

The majority of 2030 applications will operate elastic without explicit resource reservations, if the experience of the last 20 year is any good indicator for future trends. The strong resource reservation based approaches with fixed bandwidth reservations in IntServ/TSN/DetNet is not required for these, and therefore their guaranteed maximum bandwidth guarantee mechanisms are also not applicable (as it depends on known reserved bandwidths).

Nevertheless, more and more 2030 traffic will require lower and often also differentiated latency.

The first steps for this are the efforts in the last decade to reduce 'bufferbloat' in TCP congestion control to minimize best-effort traffic latency, and even more so the evolution of 'low-latency' transport protocols such as DCTCP [RFC8257] for lower-than-best-effort latency. Only in the past few years have the first proposal for mechanisms evolved that also allow for these different types of traffic to co-exist without per-flow-forwarding plane state (e.g.: "PI^2 : A Linearized AQM for both Classic and Scalable TCP"), allowing to build networks with e.g.: both TCP and DCTP without bandwidth reservation for the DCTP traffic.

Whereas mechanisms such as PI^2 can (only) better manage latency classes of traffic (e.g.: TCP/DCTCP) under congestion, explicit management of end-to-end latency in the per-hop forwarding without per-flow state has potentially even more fine-grained latency differentiation benefits:

Differential latency of paths are not compensated for by the network, leading to differences in congestion control managed throughput, problems with reordering and endpoint buffering in multi-participant applications ("coordinated communications") and multi-path flows (MPTCP or dual-path resilience).

Congestion caused latency is not compensated for later on in the path, in paths with multiple congestion hops (such metropolitan aggregation ring networks), differential latency between packet statistically increases (lucky packet vs. "biggest looser" packets experiencing worst congestion on multiple hops).

Absolute min/max desired end-to-end latency Service Level Objectives as defined in FGNET 2030 SubG2 cannot be specified with existing mechanisms and therefore also not be used to deal with the path issues described.

Recent research is proposing per-packet forwarding mechanisms to support the FGNET 2030 SubG2 High-Precision Communications requirements. See [LBF] "High-Precision Latency Forwarding over Packet-Programmable Networks" to appear at IEEE NOMS , April 2020.

14.5.4 Resilience Techniques and Near zero-loss QoS

Today's networks offer protection against packet loss primarily via two mechanisms, one at the link layer and the other at the network layer. In each case, the target QoS is maintained using proactive recovery (resilience) techniques.

At the link layer, proactive redundancy such as Forward Error Correction (FEC) is used against link bit errors such as in ADSL/VDSL, directed radio links or 100 Gbps Ethernet and beyond to achieve a desired low-level of lost packets (typically < 10^-12 or lower). On radio links including 5G/B5G, WiFi or directed radio links, reactive redundancy such as retransmission is used to overcome less well predictable loss such as temporary radio impairment. This typically leads to negligible loss in most fiber based links, but often relevant amount of increase in latency and temporary throughput for other, especially radio links.

While it is possible to expose worse than perfect links to the network layer and take those link properties into account for the path selection of different types of traffic, this is not provided as a part of the services in today's networks. Whether this is relevant in 2030 networks depends primarily on how many non-perfect links, such as microwave connections, will be in relevant 2030 networks. With the ever more omnipresence of fiber links, this may not be a relevant issue, but likewise, there is also a trend for more transit links using radio technologies (not only for mobile access), and those links would be much better useable if the end-to-end network service QoS would support distinguishing routing or even just retransmission across them for traffic that can or cannot sustain specific levels of loss. For example, TCP best effort traffic (without latency requirements) can well deal with sub-percent packet loss and therefore leverage such non-perfect links much better than traffic with higher QoS requirements (primary lower latency).

At the network layer, today's approach to component failure and recovery (link, interface, linecard, node) is at best via reactive rerouting, which typically achieves in the order of <= 50 msec interruption and recovery through technologies typically called Fast Re-Route (FRR). This level of recovery was recognized to be detectable in voice transmission over TDM but was also shown to be indistinguishable from even longer outages such as < 1 sec interruptions for real-time streaming of video with Group of Picture (GOP) sizes of 1 second – because with a significant probability, a single packet loss can invalidate a complete GOP. In result, one of the main design criteria in networks for real-time services is not primarily to minimize the time of loss and recovery but to minimize their occurrence through the choice of reliable components, internal redundancies in components and resilient make-before-break network operation procedures. Often interruptions for example are caused by break-before-make reconfigurations.

To support at the network layer less than this sub 50msec loss without the addition of latency through retransmission or FEC, it is necessary to transmit data multiple times across network paths without common failure points. This is called path-diversity and the approach of sending traffic multiple times is called (for example) live-live or seamless protection switching as in broadcast video solutions using SMPTE 2022-7. The basic principle is to send each packet twice across diverse paths and eliminate the duplicate packets (when there is no loss) based on sequence numbers.

While such live-live services exist today in a variety of private network or private network services (broadcast video industries, financial industries), there is no standardized framework/protocol/signalling to request such a service experience over two access interfaces into a network, and there are no easy to deploy and widely available routing solutions to support to support this zero-loss solution. For example, RFC8711, Maximum Redundant Trees (MRT) is one available IETF standard that can support this service from the routing perspective, but its main goal was not to enable live-live service but instead just the sub 50…msec FRR, and for that solution a wide variety of alternatives exists, so the key unique benefit of the MRT solution to enable live-live services was not widely recognized. Nevertheless, being distributed,

RFC8711 being distributed, its results for path latency are not as good as central PCE controller calculated live-live path sets.

In summary, one key recommendation for (near) zero-loss QoS in 2030 networks is to build a comprehensive resilience architecture that enables turnkey use of multi-path redundancy for critical, low-latency applications, alongside traditional link layer methods such as FEC at the link layer (see also section 2.8 on Resilience in Principles, and section 11.2.4 on Assuring QoS and Resilience in Management).

14.6 Dependencies

Past experience has shown that advanced in-network functionality face the greatest challenge in the dependency between the customer desiring these functions for applications, the network operator attempting to monetize the new functionality, and the equipment vendor attempting to finance the often necessary development of new hardware to support this functionality.

In the past two decades these dependencies worked out best when the customer was the operator, so that only two entities where involved in realizing the solution: The network + application owner/operator and the equipment vendor. Likewise, owners of applications became network operators themselves when they could get equipment with the required functionality but no operator to offer it: The fewer parties involved the more likely it did happen in networking.

Software-ization through VNF/NFV changes and improves this difficult equation dramatically, as can be seen with the large amount of mostly-software based (overlay/VPN/SD-WAN) network services that emerged in the last decade, software-ization of Central Offices of Service Providers (eg.: CORD) and so on.

The following sub-sections describe key areas of dependencies and proposals for solution.

14.6.1 Programmable virtual networks

Programmable virtual networks are a key solution option to allow future network 2030 application owners/operators to drive their required end-to-end solution without the aforementioned problems of aligning with physical network operators or equipment vendors. Programmability allows to ensure that all required functionality can be supported and virtual allows to share a common, cost effective underlying physical network infrastructure.

Initial stages of this direction can easily be seen in the mostly softwareized overlay network solutions prevalent in SD-WAN, and are foreseen to extend into the network 2030 interesting metropolitan size networks where distributed Edge-data-centers can host the VNF/NFV forwarding planes of such application specific virtualized networks.

Nevertheless, when it comes to QoS, it will arguably not be sufficient to only embody the required functions only in VNF/NFV in edge-data-centers, but it will also be required on the Multi Tbps network forwarders forming the physical infrastructure of the metropolitan networks, because they determine that latency and throughput between any two points (users, devices, edge-data-centers).

When it comes to programmable forwarding planes, some initial industry wide available mechanisms exist, driven by the need for programmable data planes in Data-Centers for example via the P4 programming language that still today primarily targets that market segment.

14.6.2 Reusable, extensible forwarding protocol packet formats

For current network forwarding plane hardware, the mayor challenge for a network 2030 strategy as outlined here is their inability to scale to support a sufficient number of separately programmed virtual network contexts to allow operating multiple independent virtual network contexts.

If each virtual network was to re-implement a network forwarding protocol stack from scratch the total required context would be too expensive. A simple comparison of this problem to general purpose CPU here is the total amount of L1/L2 cache in general purpose CPUs, and the drop in performance which would be inacceptable for packet forwarding if the code side would exceed those caches.

To solve this problem, virtualized networks will require a common network packet forwarding framework, where individual virtual networks would only need to pick and choose required subsets of widely adopted network packet features and only add new forwarding code for functions/actions that are novel to this virtual network.

One proposed framework for such extensible, reusable network packet formatting to support new services is called "Big Packet Protocol", see "Packet-Programmable Networks and BPP: A New Way to Program the Internet" in the tutorials of the IM2019 conference.

14.7 High speed programmable forwarding plane QoS

The programmability challenges for QoS go beyond the aforementioned programmability scalability and efficiency challenges for other components of the forwarding plane of network devices.

QoS support in even todays programmable forwarding planes is most often based on long-time established fixed functionality building blocks with a range of configurable parameters: Hierarchical DiffServ QoS with per-class programmable assignment to Queues and drop-behaviour in queues, assignment to per-flow Queues with similar parameters to name the most common functions.

This functionality is insufficient to allows programming of any of the aforementioned scheduling disciplines or AQM mechanisms or the LBF high-precision communications. Even within proprietary programmable vendor specific forwarding plane chips, QoS is also more ossified than other parts of network packet forwarding because of the absence of well established, more flexible programming models than above mentioned configurable 'legacy-QoS' toolset.

Only in lower end forwarding planes with for example FPGA is it possible to implement flexibly new scheduling disciplines today. This was done for example more widely in ethernet switches attempting to support the wide range of competing (proprietary) time sensitive ethernet options and resilience options (redundant L2 rings). Nevertheless, FPGA in general are considered to be too expensive and consume too much power in high-speed networking equipment.

Solving this problem is therefore an active area of research, and has produced in the past years recommendations such as Push-In-First-Out (PIFO) and Push-In-Extract-Out (PIEO) queuing disciplines to allow programming new QoS disciplines by combinations of these queuing disciplines and per-packet programmed forwarding code on packet enqueue and dequeue.

While these approaches look very promising in enabling a wide range of future-proof programmable QoS, it still has to be seen if they can be implemented at cost in Tbps hardware, especially when being implemented in a fashion where they are not limited to support only a limited number of flows. The aforementioned LBF QoS discipline in support of FGNET 2030 SubG2 requirements has also been validated based on these queuing disciplines.

14.8 Monetization

Today, monetization of differentiated QoS for different traffic is limited to private networks, such as potential different charging for different classes of traffic in L3VPN services. There are only few and ad-hoc pricing differences for different QoS services beside the ubiquitous "peak bitrate" charging for Internet services, and in less developed countries still the "Volume charging". Exceptions include sometimes statically charged overall lower latencies such as over xDSL.

Monetization is an important dependency for making future QoS services successful in networks, but it is outside the scope of this document to provide guidance.

14.9 QoS and mobile networks

This section summarizes the evolution of mobile networks from 4G/LTE to 5G and puts it in perspective to transport network QoS.

14.9.1 LTE Networks QoS Analysis

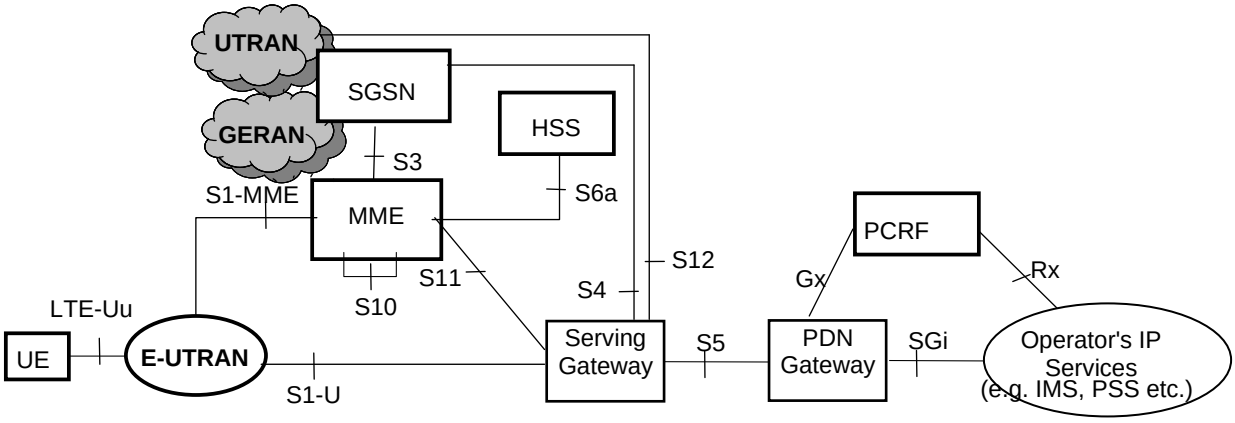


Figure 59- LTE Architecture [QoS.10]

[QoS.1] lays out the LTE architecture and is shown above for the QoS discussion. QoS and user profile of the UE is enforced in service end points E-UTRAN, Serving Gateway/PDN Gateway. Though various bearer types with different QoS requirements were defined in LTE specifications only default bearer and voice bearer are deployed predominantly. Transport network is between E-UTRAN and S-Gateway on S1-U interface and S-Gateway and PDN Gateway on S5 interface. Here, user data traffic is encapsulated with GTP-U overlay with mostly IP and MPLS undelay technologies.

Default bearer corresponds to data traffic for internet access and would be treated in best effort manner in the transport network. To provide the QoS for the UE packets at E-UTRAN in the down link direction and S/P-GW in uplink direction, IP packet DSCP fields are copied in the outer IP header after GTP-U encapsulation. If MPLS is used in the transport network, then IP DSCP to MPLS EXP bit mapping would be done. The need for QoS in the transport network itself is primitive and basic prioritization of the voice packets is generally deployed to mitigate the congestion in the transport network.

14.9.2 5G Network QoS Analysis and new Requirements

[ROUT.21] describes the system level architecture of the 5G network and is shown below for QOS discussions.

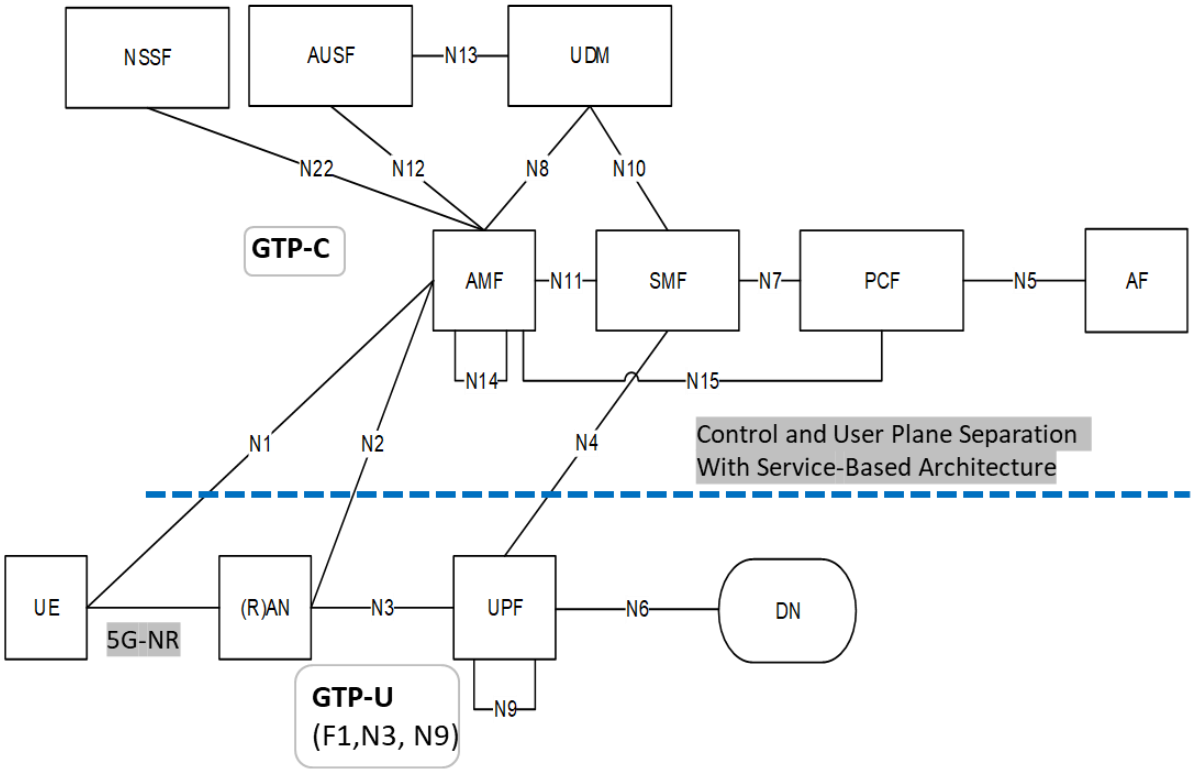


Figure 60- 5G Architecture [ROUT.21]

While there are lot of changes in (R)AN and the 5G control plane from LTE, significant difference w.r.t QoS from service level is required because of the slicing requirements in 5G networks. An end to end slice is defined as slice in (R)AN, transport network and Core network. To meet the slice characteristics w.r.t QoS, resiliency and hard separation, transport network need to be factored unlike in LTE.

Transport network can be defined between (R)AN and UPF on N3 interface. This is like S1-U and S5 interface in LTE at high level. Another part of transport network is N9 interface i.e., the network between multiple UPFs. This is a new architectural interface and has designed to address multiple requirements in 5G from URLLC, Session offloading and new Session and Service Continuity (SSC) modes as defined in [2]. QoS characteristics for each slice need to be provisioned, applied and honoured for the data traffic passing in the transport network in the respective segments wither on N3 or N9 interface. QFI parameter in the GTP header describes the PDU session QoS requirements. Based on the SST in S-NSSAI in 5G control plane, QFI value would be set in the 5G service nodes i.e., (R)AN, UPF in uplink and downlink directions respectively.

An example mapping for QFI, SST and transport path is shown below:

GTP/UDP SRC PORT (mapped to 5G dynamic QFI)	SST in S-NSSAI	Transport Path Info	Transport Path Characteristics
Range Xx - Xy X1, X2 (discrete Values)	MIOT (massive IOT)	PW-ID/VPN Info, TE PATH-X	GBR (Guaranteed Bit Rate) Bandwidth: Bx Delay: Dx
Range Yx - Yy Y1, Y2 (discrete Values)	URLLC (ultra-low latency)	PW-ID/VPN Info, TE PATH-Y	GBR with Delay Requirements Bandwidth: By Delay: Dy Jitter: Jy
Range Zx - Zy Z1, Z2 (discrete Values)	EMBB (Broadband)	PW-ID/VPN Info, TE PATH-Z	Non-GBR Bandwidth: Bx

Figure 61- Mapping Table for 5G Slices to underlying Transport Paths

The delay and jitter defined above are part of the QoS profile for that slice. The QoS state here is per traffic engineered path and UE PDU sessions need to be mapped based on slice specific criteria to these QoS Paths.

There are considerable gaps to achieve the QoS requirements in transport networks in 5GS, as some of the requirements purely belong to transport domain and is not governed by 3GPP. Transport Aware Mobility for 5G [3], discusses how a standardized mapping from 3GPP domain to transport domain can be done and gaps in available technologies from transport side w.r.t QoS.

14.9.3 B5G QoS Requirements

There are some initial discussions in various forums on B5G and this is an evolving topic. Transport network characteristics for these networks need to be understood and be factored upfront for mission critical applications requiring future network support.

14.9.4 Mapping 5G/B5G to the underlying Network 2030 infrastructure

In the most simple instance, a 5G, and likely B5G network can be mapped onto the previously explained Network 2030 infrastructure solely as an “overlay” network, where all control-plane and user-plane functions are running in edge-data centers as VM/Containers or even lamda implementations. Even if some functions are still requiring specialized hardware, such as NPU processing, they would till very likely be positioned solely in edge-DC.

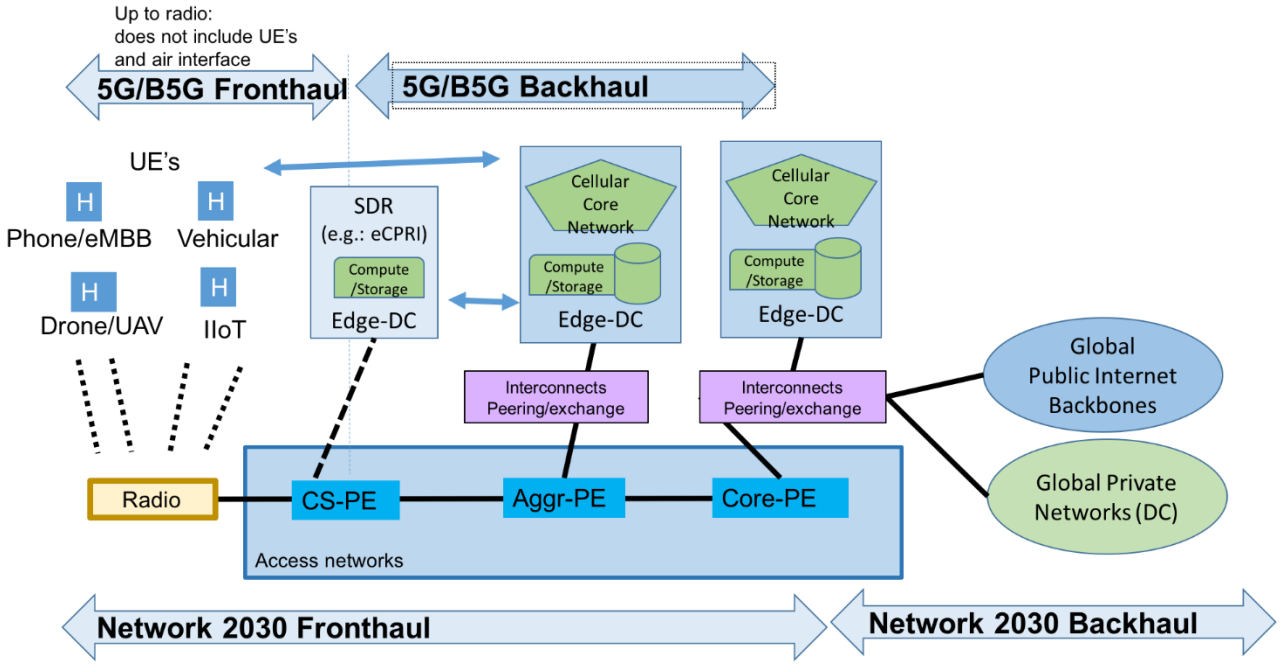


Figure 62- 5G/B5G Fronthaul and Backhaul

The above picture outlines how the 5G/B5G functions would integrate into the Network 2030 fronthaul. The Network 2030 fronthaul access network is the 5G/B5G transport network representing N3, N9 and N6 in the 5G architecture. When 5G functional blocks are distributed across multiple edge-DC in the network 2030 fronthaul, then other Nx could also run across the underlying transport network, otherwise they would solely run between compute units providing VM/container/lambda to the 5G/B5G solution.

In today's assumptions, Nx interfaces that pass through the network 2030 fronthaul access networks would need to be subject to QoS services described in this document. Nx interfaces that solely pass within the same Edge-DC may considered to always have negligible latency and no congestion relevant to the provided service. These assumptions may not hold if for example Deterministic Services or high-precisions services are required across 5G/B5G, in which case burst-collisions even within a DC could be detrimental to the required service, and QoS services would also need to extend into the Edge-DC internal networks.

The use of slices in 5G/B5G can be independent or coupled with similar isolation mechanisms in the network 2030 fronthaul access networks. This is subject for further study.

Beside 5G/B5G, there is also the question of supporting software-ized radios, as feasible via eCPRI [QoS.3] or future techniques evolving from it. It is highly desirable to enable supporting this functionality such as any other (software) service, but it comes with likely todays most strictest latency and jitter requirements such as a one way path delay of no more than 25 usec. With the evolution of access network switching speeds from 100 Gbps to beyond (Tbps or more), the latency of the actual network equipment should not be a key impediment to this goal, but the speed of light will still limit the access to likely at most one or two active switching components between the radio hardware device and the compute element. Hence, the above picture shows this option as one requiring a compute component that logically needs to be closest to the subscriber/radio edge, considered to be part of the 5G/B5G fronthaul.

The specific beneficial QoS service attributes for eCPRI (or successor) traffic are subject for further studies, but it seems clear that even a single switch that is connecting multiple radios with a single compute node would potentially have to deal with the problem that traffic arriving from those multiple radios (each from a different interface) could create undesirable FIFO burst collision delay when queuing towards the compute node and that fully synchronous solutions are likely raising the cost of the solution undesirably.

15 Burst Switching

The burst forwarding is an application-aware data forwarding technology. A burst is the basic data unit that can be processed by the application. The content of the burst is application dependent. For example, a burst can be a photo in the image processing system, or it can be a video clip in the video streaming service. The burst forwarding network uses burst as the basic transmission unit. The data source sends the entire burst using the line rate of the network interface card (NIC). End to end virtual channels are created for the burst transmission. In the burst forwarding network, the burst are forwarded using cut-through and the data forwarding is congestion free. In the receiver side, the application usually needs to receive the entire burst before start processing the received data. If the application data are received in packets with multiple flows, the application needs to buffer the data until the whole burst is received. In the burst forwarding network, however, the application data are received in sequence. The application in the receiver node can immediately process the data without any further data buffering. This mechanism not only accelerate the burst data end to end transmission time, it also optimizes the computation resource utilization of the data processing.

This document presents the architecture design of the burst forwarding technology. The use cases and the problem analysis are firstly presented in chapter 15.1. The category of the applications that can benefit most from burst forwarding technology are also described. In chapter 15.2, we summarized the theory study results. The necessity of using burst forwarding in the future network is discussed, which includes the analysis results of the network throughput, the end host performance, the application data processing efficiency and the router buffer requirement. Finally, in chapter 15.3, we describe the architecture design of the burst forwarding network in detail..

15.1 Motivation

The current network is a packet forwarding network. The data generated in the applications are usually much larger than the packet MTU size. Before transmitted to the network, the application data is segmented and encapsulated into many 1.5KB packets. During the data forwarding, the packets from different flows are interleaved in the congestion link. Congestion control algorithms are designed to equally share the congestion link bandwidth between different flows. In the receiver side, the application needs to retrieve the entire application data to start processing. In a congested network, the data transmission time in the network could be much longer than the data processing time in the receiver node. In this case, the computation resource utilization rate in the receiver node is very low. Additionally, uncorrelated data transmission in a bandwidth converged network usually has incast problem. The packet loss due to router buffer overflow also reduce the network utilization. As a result, it takes even longer time to finish the data transmission.

If burst forwarding technology is utilized, each application related data is transmitted to the destination node in sequence. The application in the receiver node can immediately starts the data processing in pipeline. Therefore, the computation resource utilization in the receiver node is optimized. Moreover, by carefully arrange each burst transmission, the network controls the ingress traffic to never excess the network egress capacity. In this case, the network can be congestion free.

This section describes two use cases in detail. The metro gate control using face recognition system and the video surveillance system with real-time image processing. Simulation result of computation resource utilization and data transmission latency are presented while running TCP network and burst forwarding network.

15.1.1 Use case description

15.1.1.1 Metro gate control face recognition system

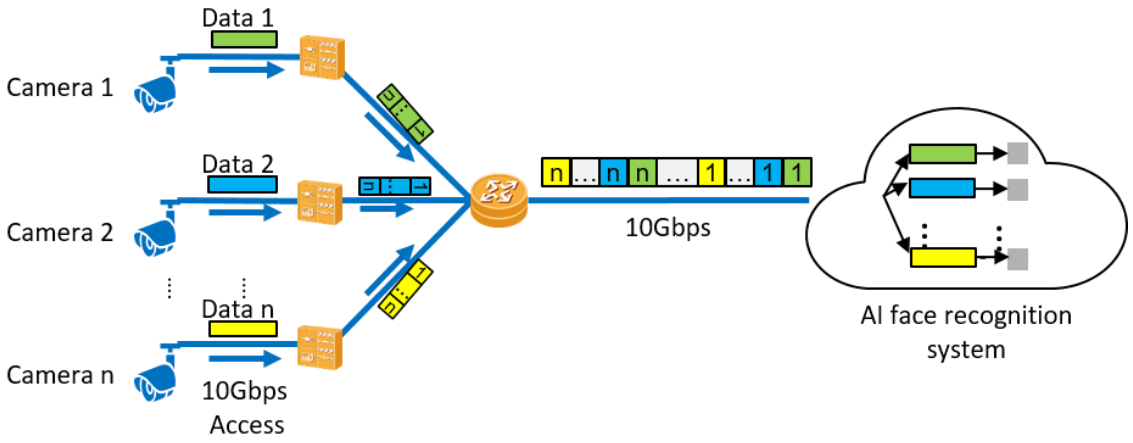


Figure 63- Metro gate control face recognition system architecture

Figure 63 illustrates the sample network architecture of the metro gate control face recognition system. In order to guarantee the high recognition accuracy, the metro gate camera takes high resolution picture for each passenger. The average photo size generated by the camera for one passenger is around 8MB. The cameras connect with the cloud AI system using 10Gbps leased lines. The recognition result should be sent back to the metro gate within 200ms after the photo is taken. The timing details of the system are shown in **Table 2**.

Total Time	AI	Tx	Data Size	BW per gate	Access BW	No. of lines
200ms	7ms	193ms	8MB	332Mbps	10G	30

Table 2. Latency requirement of the metro gate control face recognition system

The average serve time for each passenger should below 1.5s. Within which, 1.3 s are consumed by the door open (0.3s), the passenger pass through (0.7 s) and the door close (0.3s). The rest 200ms can be used by the end to end network communication and data processing. The face recognition service consumes 7ms to process a photo per network processor core. Therefore, the maximum end to end data transmission time is 193ms. The physical bandwidth of the cloud access is 10Gbps, which can support 30 concurrent photo transmissions.

Problem analysis:

The AI face recognition service cannot process partially received photo. It needs to wait until the full photo to be received. As shown in **Figure 64**, if all cameras start sending photo at the same time, ideally, the 30 flows will be fully interleaved packet by packet. 30 concurrent photo transmission takes 193ms to deliver 8MB photo over a 10Gbps link. In this case, the AI cloud service has only 7ms to process 30 pictures. Therefore, the cloud service needs to reserve 30 NP cores for the upcoming data processing. However, during the data transmission period, no data are received in the AI cloud, the NP cores are left idle. The efficiency of AI computation resource utilization rate is only 3.5%.

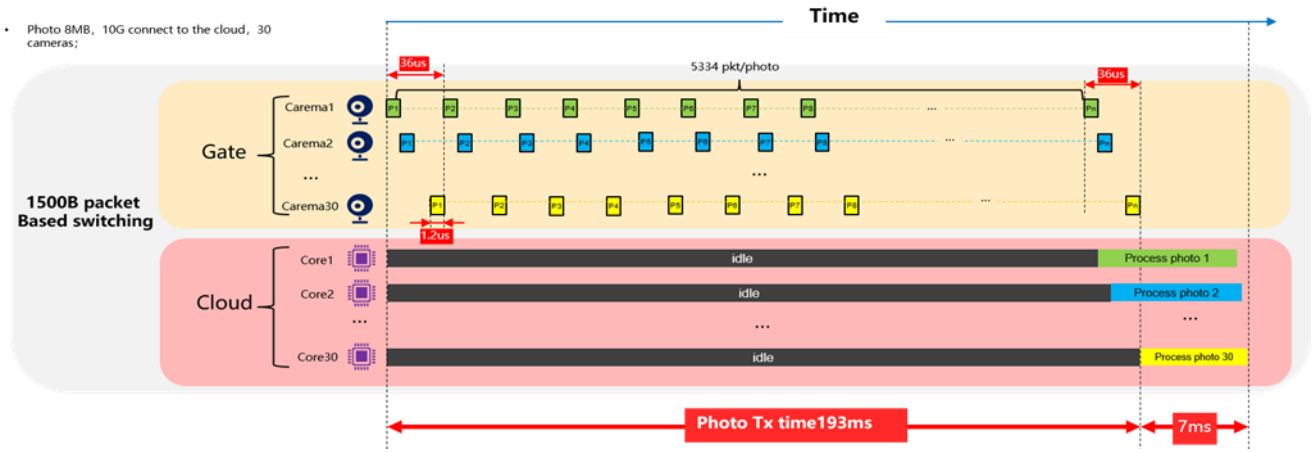


Figure 64- Computation resource consumption of 30 concurrent photo transmissions.

If the burst forwarding technology is utilized, the network forwards each photo at a time. The photo can be received by the AI cloud service much faster. As shown in **Figure 65**, every photo transmission occupies the entire bandwidth. For a 10Gbps link, it only takes 6.4ms to transmit one photo. Once the photo is received by the cloud service, it can be immediately processed. Since each core takes 7ms to process one photo, it requires maximally two NP cores to process the data. The computation resource utilization in this case is 54.6%.

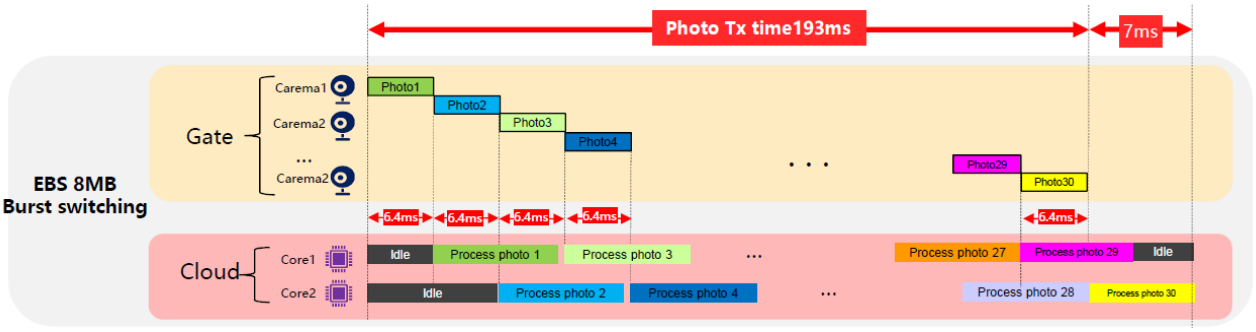


Figure 65- Application-aware data forwarding

The scenario described previously is the worst case which assumes that all the cameras sends data at the same time. We have done simulations where the photo arrives traffic pattern is configured as poisson distribution. As shown in **Figure 66**, in the packet forwarding network, more than 60% of the traffic failed to meet the 200ms deadline. The latest photo was received at 260ms. During this period, up-to 5 NP cores are needed to process the concurrently received photos.

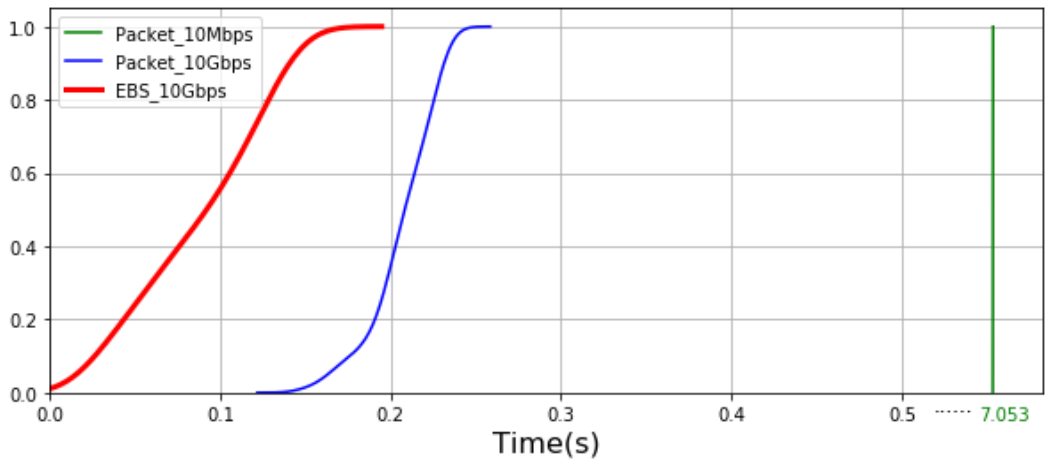


Figure 66- CDF plot of the photo arrival time.

15.1.1.2 Video surveillance system with real-time image processing

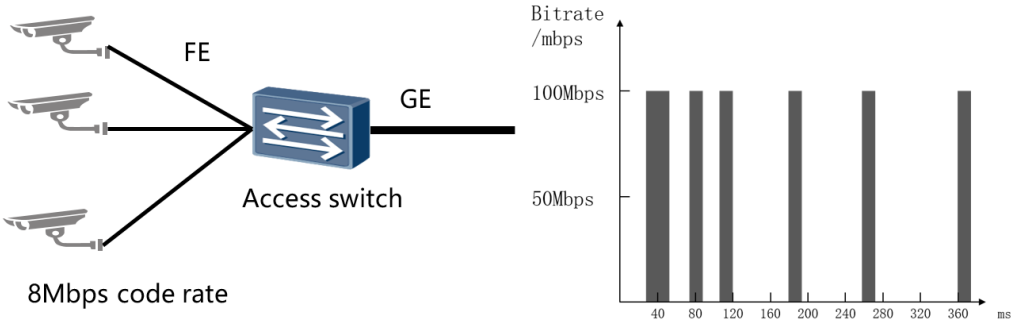


Figure 67- Video surveillance system data uploading

The video surveillance system uploads the video clips filed from different cameras to the remote server, where, the received video streams are analysed in real-time. The data generated from different cameras are required to be uploaded to the remote server within 1s.

As shown in **Figure 67**, the camera access the network using FE link. The average code rate for one camera is 8Mbps. The egress port rate of the access switch is 1Gbps. In theory, such a switch can support 125 camera connections. However, based on the field test result, the switch can only support 30 cameras without losing any packet. The equivalent bandwidth consumption is only 24%.

Problem analysis:

As shown in **Figure 68**, the cameras access the network using FE port. The GE egress port can only support 10 concurrent camera data transmission. If there are more than 10 concurrent transmissions, the switch buffer starts to store the overloaded data. The access switch usually have very shallow buffer. It is easy to lost packet due to buffer overflow. Although TCP will guarantee a reliable delivery, the retransmission mechanism consumes extra time and thus reduce the transmission speed.

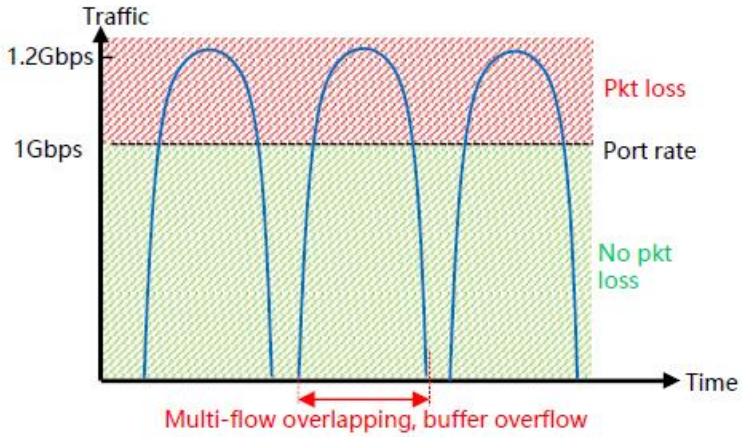


Figure 68- Packet loss due to uncoordinated multi-flow overlapping

While using burst forwarding technology, dedicated virtual channel are created for each video clip transmission. If there are more data needs to be transmitted, the burst needs to wait for the previous burst to finish data transmission. In this case, the burst forwarding network limits the number of concurrent data transmission never above 10. The accumulated ingress speed will never excess the egress speed. No packet will be lost due to buffer overflow. **Figure 69** shows the CDF of the data arrival rate with 110 camera connections. By using burst forwarding technology, all data can be delivered from the camera to the remote server within 1 second. However, when using TCP to transmit the same amount of data, more than 55% of the data failed to meet the deadline.

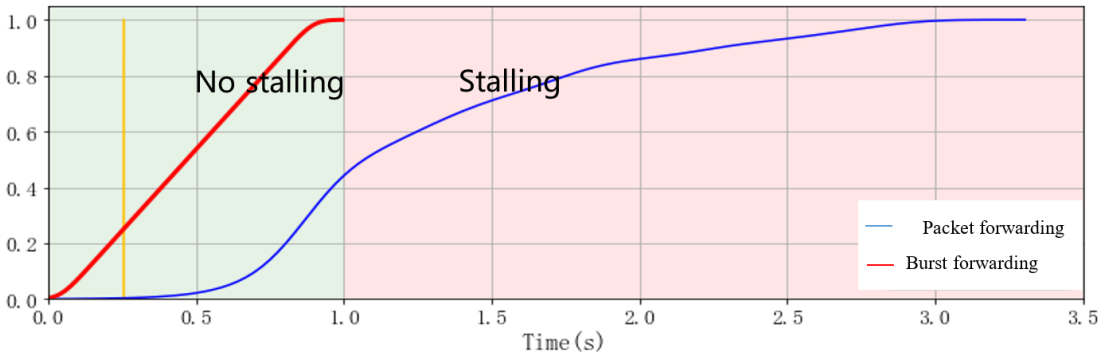


Figure 69- CDF plot of video chunk uploading interval.

15.1.2 Scope of burst forwarding technology

Based on the previous description, we further generalized these use cases into a use case category, aka, multi-source convergence with large data chunks under bounded latency. Such kind of applications usually share the following common characteristics.

- Application data are **originated from different data sources**. However, the generated data are centrally processed, e.g., in a remote cloud service.
- The network architecture of the application is usually **aggregation tree** with converged bandwidth. The accumulated physical bandwidth of all the data source is much higher than the access bandwidth to the cloud. However, the equivalent code rate match the cloud access bandwidth. The data sources use high bandwidth to access the network, but only transmit data sporadically.
- The data transmission needs to be finished **within a bounded latency**. Overdue data are either too late to be useful or it might break the pipeline of a closed loop control system.

Such network architecture are firstly noted in most of the IoT applications. Numerous amount of sensors keeps reporting measurement results to the remote server. The actuators are manipulated by the post-processing results from the remote server, for example, an indoor climate control system. However, the challenges starts emerging when the data being uploaded becomes larger and larger and the latency requirement becomes more and more tight.

15.2 Theoretical analysis of burst forwarding mechanism

This chapter summarizes the theory study results of burst forwarding network. The benefit of using bust in the current network is theoretically analysed. The analysis result shows the increment of the network throughput, the end host performance and the application data processing efficiency. We also analysed the router buffer requirement of the future large bandwidth application, e.g., holographic type of communication.

Firstly, the relationship between TCP network throughput and burst size is presented. The theory study result shows that increasing burst size can significantly improve the network throughput. The end host performance study reveals the relationship between PPS (packet per second) and CPU resource allocation. A mathematic model is built to describe the packet transmitting and packet receiving process. In the end host operating system, using small packet size triggers excessive packet tx/rx interrupts. In the worst case, the host CPU can be completely occupied by the interrupt service handling and leaves little resource for other applications. In the data transmission complete time study, we utilized the queue theory on the burst level. It shows that the entire burst receiving time is minimized when the bursts are transmitted in sequence without any interleaving. In the router buffer requirement study, we present the relationship between the router buffer consumption and bandwidth requirement. Based on the current data transmission technology, the future ultra large bandwidth applications will require too much router buffer which is difficult to be fulfilled. A new congestion free data forwarding method needs to be utilized for the near future ultra large bandwidth applications.

15.2.1 Network throughput study

According to [1], the TCP reno network throughput can be calculated using eq.1. The MSS is the burst size, RTT is the round trip delay time, ρ is the packet loss rate. At the first glance, the network throughput is proportional to the MSS size in a fixed RTT network.

$$\text{Throughput} \approx \sqrt{\frac{3}{4}}\frac{MSS}{RTT\sqrt{\rho}} \qquad \text{(EQ.1)}$$

However, the MSS size also affects the RTT value and packet loss rate. For the store and forward network, the RTT time is increased since the router needs longer time to receive the whole burst before it can be processed and forwarded. According to [2] and [3], the packet loss rate also increases when the MSS size increases. By taking all these considerations, eq.1 can be further expanded as

$$\text{Throughput} \approx \sqrt{\frac{3}{4}}\frac{MSS}{\left(\sum_{i=1}^{N}\frac{MSS}{R_i}+T_p+T_c+T_q\right)\sqrt{\sum_{i=1}^{N}\frac{MSS}{B_i}+MSS\cdot\rho_{bit}}} \qquad \text{(EQ.2)}$$

Where Ri is the link rate, N is the hop number of the path, T is the sum of the propagation delay (Tp), the computation processing delay (Tc) and the packet queuing delay (Tq). ρ is the link error rate and B is the router buffer size. According to eq.2, the network throughput reaches maximum when $MSS = \frac{T_p+T_c+T_q}{\sum_{i=1}^{N}\frac{1}{R_i}}$.

Figure 70 shows the relationship between the MSS size and the network throughput. The path consists of 8 hop, the link rate is 1Gbps, router buffer is 10 MB, Tp = 0.5ms, Tc=5ms, Tq=20ms and bit error rate BER is 10^{-12}. The throughput reaches maximum 300Mbps when MSS $\approx 400KB$. However, if 1.5KB MSS size is used, the throughput is only around 10Mbps.

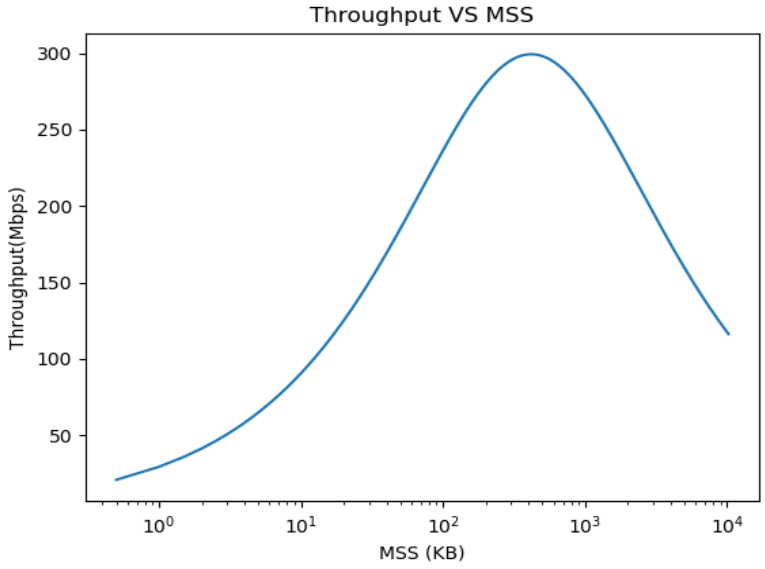


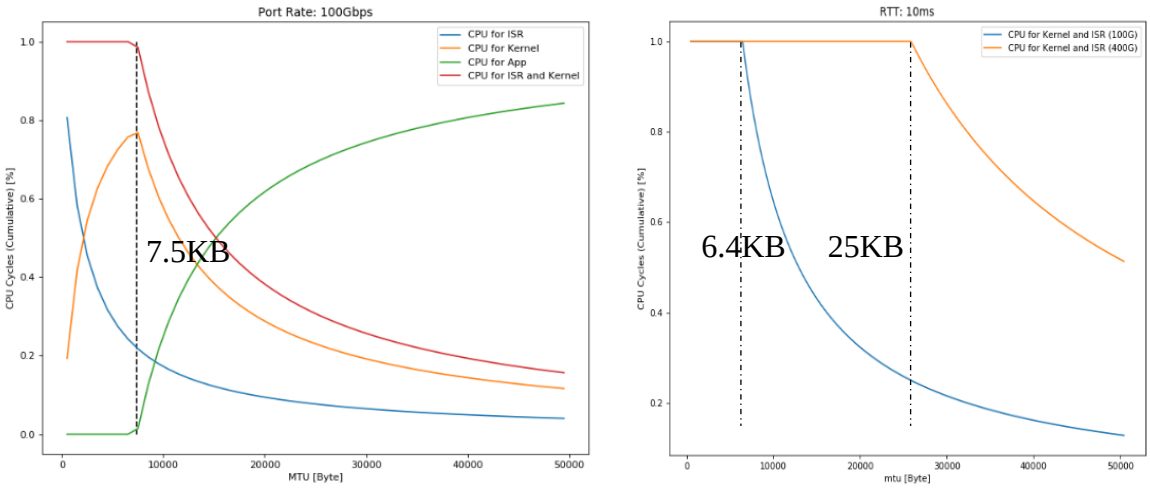
Figure 70- Relationship between the network throughput and the MSS size.

From this analysis, we conclude that using large MSS size as the basic data forwarding unit can increase the throughput of the current TCP network. However, there is an upper limit of the burst size. This problem is due to the TCP network dynamics. Larger burst result of less number of packet per bandwidth delay product (BDP). In this case, a burst loss can easily trigger network retransmission timeout (RTO) which greatly reduce the network throughput.

15.2.2 Host performance study

The PPS value has a great impact on the host side performance. Packet sending and receiving are processed in the kernel space of the operating system. These operations have higher priority than the applications in the user space. Paper [4] uses Markov state machine to create a packet receiving model. Based on the same idea, we created a similar mathematic model on packet transmission, the relations between PPS and CPU utilization are shown in **Figure 71**.

As shown in **Figure 71(a)**, when the MSS size is small, the PPS is extremely high so that all the CPU resource are occupied by the packet receiving interrupt service routine (ISR). As the MSS increases, CPU resource is released. These resource are firstly utilized by the kernel stack to process the received packets. Since both ISR and kernel stack has higher priority than the user space application, the MSS size needs to be large enough so that the CPU can have extra resource for application data processing. **Figure 71(a)** shows the CPU utilization of a server with 3.3Ghz and 100Gbps network interface card (NIC). The MSS size needs to be larger than 7.5KB so that the accumulated CPU usage of ISR handling and kernel logic is less than 100%. Similarly, as shown in **Figure 71(b)**, the burst size needs to be larger than 6.4KB at 100Gbps link and 25KB at 400Gbps during the data transmission.



(a) Packet receiving analysis

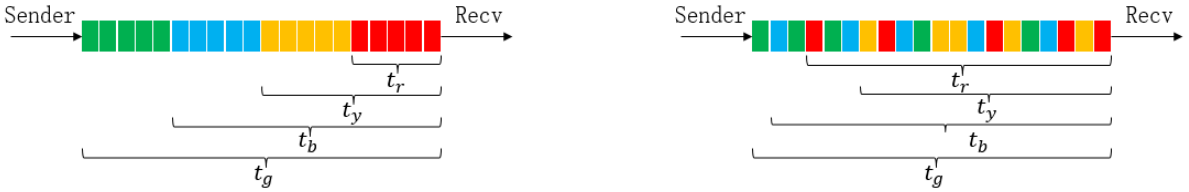
(b) Packet transmission analysis

Figure 71- Relation between MSS size and CPU utilization

Based on this study, we conclude that using burst as the basic data forwarding unit can greatly reduce the PPS. In order to save CPU resource for other tasks, it is essential to use large burst size by the end host with high NIC bandwidth.

15.2.3 Data transmission complete time study

A bust contains the application related data. The application needs to receive the entire burst to begin data processing. In order to increase the data processing efficiency in the host side, the burst needs to be received in sequence. If different bursts are interleaved, the end host needs to buffer the data until the entire burst is received. **Figure 72** shows the burst transmission complete time of different forwarding methods. As shown in **Figure 72 (a)**, the four bursts are transmitted in sequence. The total waiting time of the four bursts is minimized. If the bursts are forwarded with interleaving, as shown in **Figure 72 (b)**, a burst transmission is only completed when the last data block of that specific burst is received. As long as burst are interleaved, the averaged burst transmission complete time is not optimized.



(a) Burst level forwarding *(b) Interleaved burst forwarding*

Figure 72- Burst forwarding with or without interleaving.

This observation can be explained using the M/M/1 queue theory. We assume that there are N bursts that needs to be transmitted. The burst size is L and each burst contains small data blocks with size l. In this case, the waiting time of all the bursts is the accumulated queuing delay of the last data block of different bursts in the queue. The average waiting time of the burst can be expressed in eq.3

$$t = (t_r + t_y + \ldots + t_b + t_g)/N = \frac{(N+1)L}{2\rho l} + [\frac{(N-1)\ L}{2\rho l} - \frac{(N-1)}{2\rho}]x \qquad \text{(EQ.3)}$$

Where ρ is the data block service ratio and x is the interleaving degree. The interleaving degree is a discrete distribution indicator ranged from 0 to 1. 0 means all the burst are transmitted in sequence, while 1 means the burst are fully interleaved. When x is zero, the equation is the same as the classic queue theory which corresponds to the minimum waiting time.

Based on this study, we concluded that sending the entire burst to the destination node without any interleaving can optimize the average burst delivery time.

15.2.4 Router buffer requirement study

The router buffers are needed to ensure the high network utilization. Congestion control algorithms such as Reno and Cubic relies on the packet loss to detect the network congestion. Due to the addictive increment multiplicative decrement (AIMD) algorithm, the data transmission speed is decreased after the packet loss. The buffered data are used to compensate the low network utilization which caused by the temporary low transmission speed. The buffer should store enough data so that the sender can recover from the previous transmission speed decrement.

As shown in [5], the router buffer size which ensures high network throughput can be calculated using the following equation:

$$\text{BufferSize} = C * \text{RTT}/\sqrt{n} \qquad \text{(EQ.4)}$$

Where C is the congestion link capacity, RTT is the round tripe delay time and n is the number of uncorrelated flows / users. It is worth to note that the buffer requirement is inverse to the square root of the user number. As shown in

Figure 73, we have experienced massive user increment during the past 10 years. However, the bandwidth requirement per user only increased from 480P video to 1080P HD video. This situation will change for the next 10 years. The emerging media technologies consumes significantly higher bandwidth. For example, basic VR consumes 50Mbps bandwidth which is 8 times higher than HD video. Extreme VR consumes 15.2Gbps bandwidth which is 2500 times higher than HD video. Such great bandwidth increment also requires proportional increment of the router buffer. It is believed that the current network processor architecture can only support up-to good VR [6].

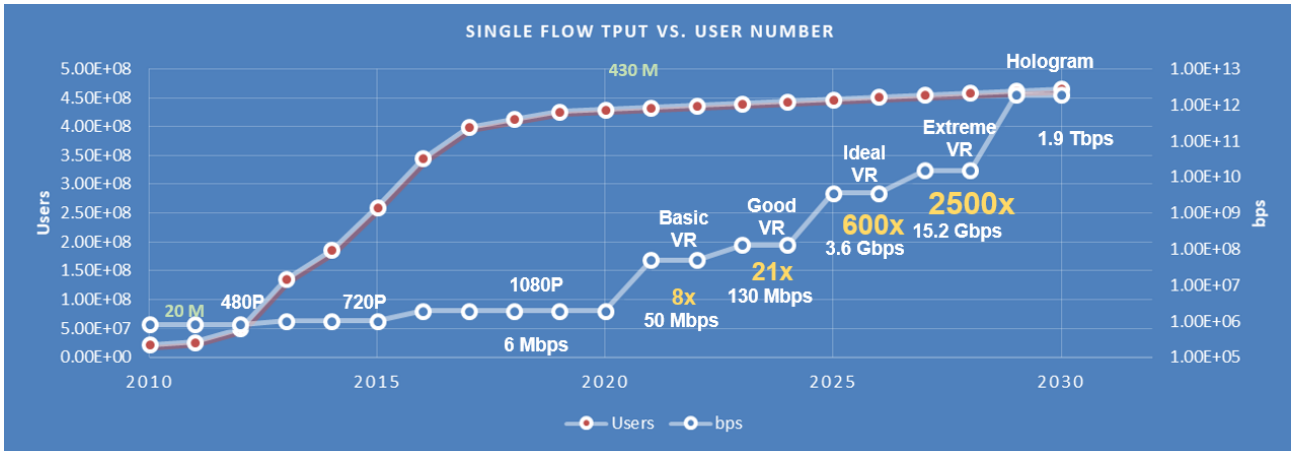


Figure 73-. Future trend of user number and the bandwidth requirement of applications

Figure 74 summarized the buffer requirement of different applications. We assume a dedicated router with 100Tbps switch capability which serves different applications every time. Based on the bandwidth requirements shown in

Figure 73, the concurrently supported user can be calculated. Meanwhile, the required router buffer size can be calculated using eq.4. As shown in **Figure 74**, in order to support HD video streaming, the router only consumes 31MB buffer. For Basic VR, 88MB router buffer is needed. As the bandwidth increases per application, the concurrent supported user number decreases. For good VR, ideal VR and extreme VR, the buffer requirement is 143MB, 750MB and 1.541GB. For the hologram, an astonishing 17.17GB router buffer is needed. According to [6], the practical NP cache size should below 256MB. In this case, the current NP technology can only support up-to good VR application.

In order to decouple the buffer usage from network throughput, a new data forwarding flow control algorithm is needed.

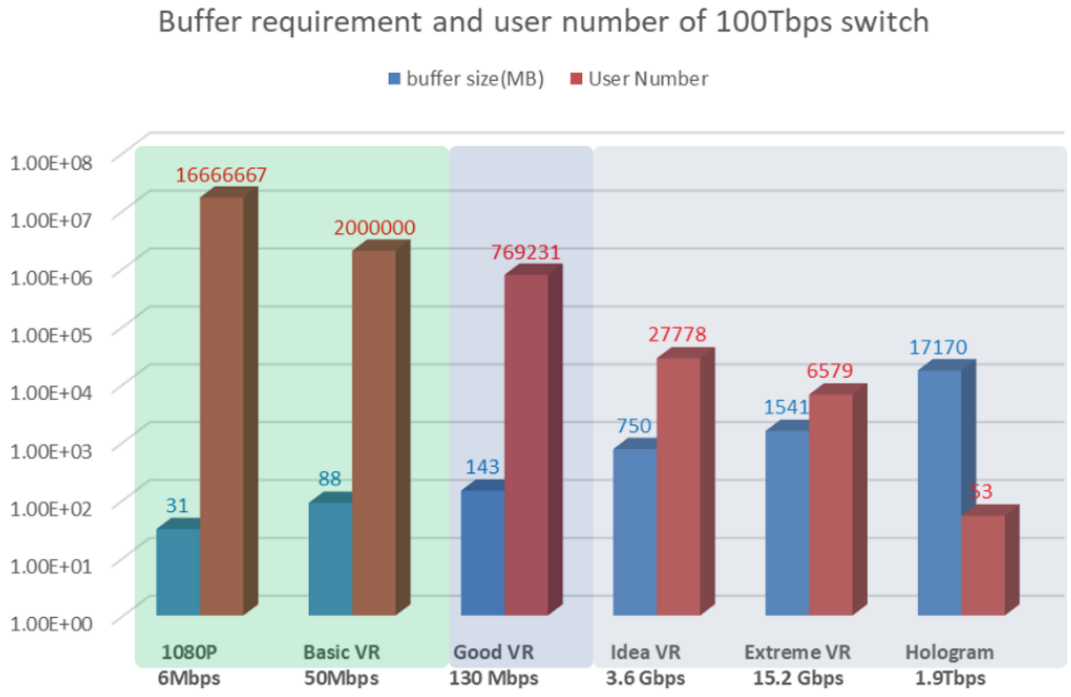


Figure 74- Buffer requirement of different applications.

15.3 Burst forwarding architecture design

The current network architecture is originally designed for packet-oriented data forwarding. Numerous efforts has been done to smooth the data transmission, evenly share the congestion link bandwidth and predict the available bandwidth and RTT. Uncoordinated burst transmission could cause severe incast problem in the current network architecture and therefore reduce network performance. However, the concept of burst forwarding network is different from the mindset of the traditional data forwarding. Instead of evenly share the bandwidth, each burst transmission occupies all whole bandwidth of the link for a short period. The network should guarantee that the burst is sent to the destination without any congestion. This chapter describes the burst forwarding network architecture design in detail.

The burst forwarding network requires the collaboration between the network side and the host side. Both sides work together to provide a burst forwarding service infrastructure. This chapter begins with the general description of the burst forwarding network architecture. The network creates virtual channels for each burst transmission to guarantee cut-through forwarding. Secondly, the data plan design is presented. When being forwarded, a burst is split into multiple small data chunks, aka burstlet. On-demand local forwarding table entries are created for burstlet forwarding. The forwarding entry are deleted once the burst is successfully transmitted. Thirdly, the host architecture consideration is described. A new data interface is proposed for burst data sending. Moreover, the host also collaborate with the burst grant send algorithm. It blocks the application data transmission until the network is free. Finally, the burst grant send algorithm requirement for burst forwarding is presented. The goal of this algorithm is to guarantee that the burst transmission is congestion free and consumes limited router buffer.

15.3.1 Architecture overview

The store and forward mechanism requires the router to buffer the entire packet before forwarded to the next hop. In the burst forwarding network, a burst can be 10x MB or even 100x MB in size. Store and forward bursts consumes huge amount of router buffer. An alternative method is the cut through forwarding. The cut through method starts forwarding a packet after the address fields were received. It is a good candidate for burst forwarding since it requires minimum router buffer. However, the limitation of cut through forwarding is that it requires the same link speed end to end. Burst forwarding leverages virtual channel technology to create path with same link speed on demand. **Figure 75** shows a sample burst forwarding network architecture.

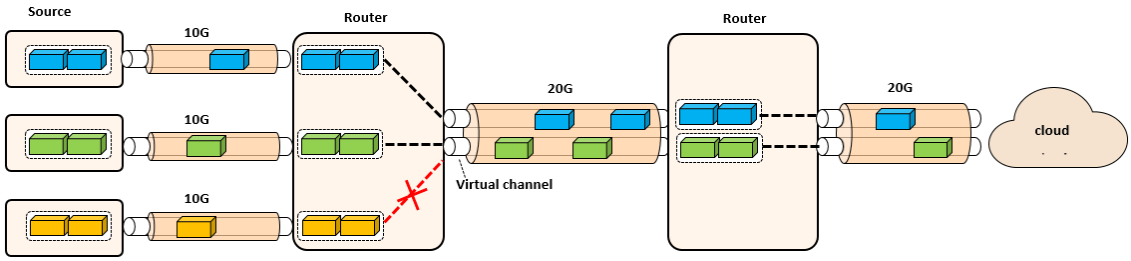


Figure 75- Burst forwarding network architecture

As shown in **Figure 75**, three data sources access the network via 10Gbps link. The access router connect to the cloud via 20Gbps links. In this case, the 20Gbps link is divided into two 10Gbps virtual links. The links can be concurrently used by any two data sources. If all the three data sources want to send burst at the same time, one of them has to be blocked until the previous transmission finishes. By doing this, the burst forwarding network guarantees that the burst can be forwarded in the path using cut through. The data can be received by the destination as fast as possible.

15.3.2 Network data plan design

Forwarding a burst in a packet oriented network has many challenges. One obvious problem is the head of line (HOL) blocking. High priority packets can be blocked by the long lasting burst transmission. In the worst case, a small packet could be blocked by the burst twice inside a switch. As shown in **Figure 76**, if a small packet and a burst are received from two different ingress ports almost at the same time, the small packet could be block by the burst before sent to the packet forwarding engine (PFE) for further processing. Moreover, if the two packets happens to be scheduled to the same egress port, the burst could block the small packet one more time. This problem could increase the service jitter and reduce the network determinacy.

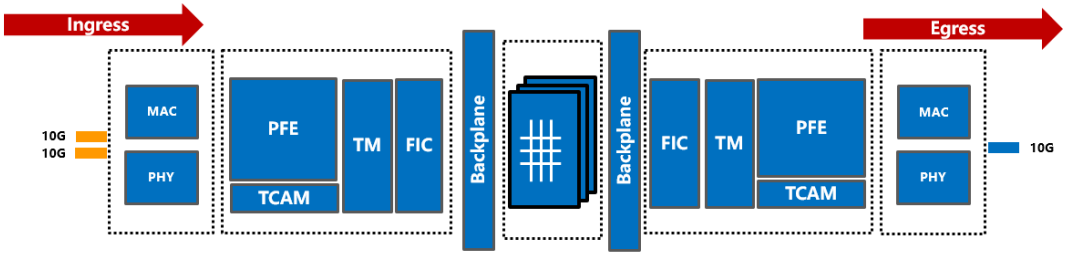
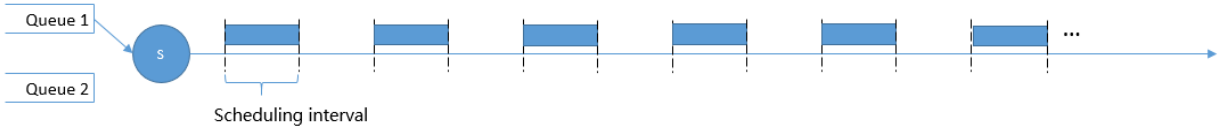
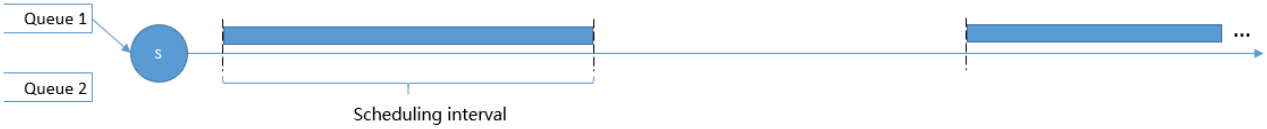


Figure 76- HOL problem of router forwarding a non-splittable burst

As another practical problem, forwarding a burst also increases the switch QoS scheduling interval. It reduces the shaping effect from the switch traffic management system. For the switch traffic management, the minimum scheduling interval should be longer than the transmitting period of the biggest frame. Since a burst takes longer transmission time, it prolongs the scheduling interval of the router traffic management. For short frames, the shaping effect of traffic management is decreased by using long scheduling interval. If too many short frames are scheduled in the same interval, it could form a microburst.



(a) Short interval for small packet scheduling



(b) Long scheduling interval for burst scheduling

Figure 77- Packet scheduling interval composition between packet and burst

To solve the mentioned problem while largely maintaining the current router architecture, we need to decouple the router basic forwarding unit from IP packet size. This section provides the high level description of this mechanism. Instead of forwarding the entire burst at once, the burst is further split into smaller data blocks, aka burstlet. The burstlets are sent in a wormhole-switching-alike mechanism along the virtual channel. In this case, the high priority small packet transmission only needs to wait for a burstlet instead of the entire burst. It also improve the accuracy of QoS since burstlet level scheduling providing finer granularity.

15.3.3 Burst data packaging

Depends on the data size, a burst is split into head burstlet, one or more body burstlets and a tail burstlet. As shown in **Figure 78**, the header burstlet includes the routing information of the entire burst, e.g., source and destination IP addresses and port numbers. The body burstlet and the tail burstlet only contains the data of the burst. The burst ID uniquely identify a burst which links the head burstlet with the remaining

body and tail burstlet. This is especially useful when multiple virtual channels shares the same physical link where burstlet from different burst are interleaved.

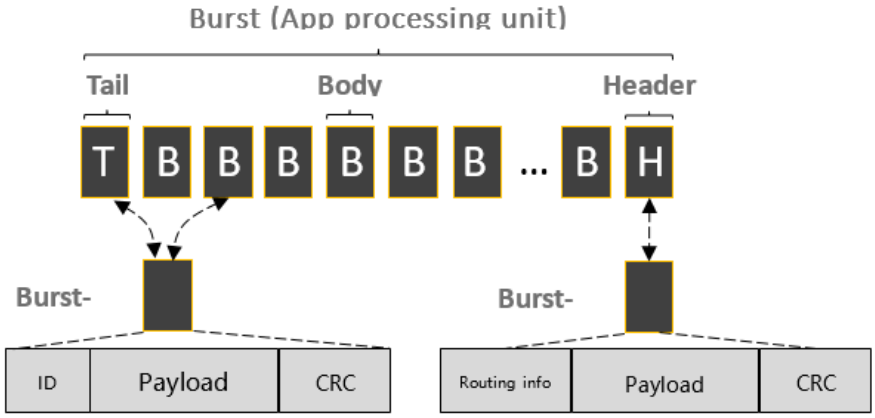


Figure 78- A burst consist of head burstlet, body burstlet and tail burstlet

Typically, a burstlet should include the following information in order to be correctly forwarded:

Datatype: Flags indicating the type of the burstlet, i.e., head, body or tail burstlet.

Burst ID: Uniquely identify a burst from the same data source.

SEQ: Burstlet id within a burst. Used by the burst receiver host for reliability check.

Port rate: Identify the sending speed of a specific burst. Carried in the head burstlet to create dynamic virtual channel.

15.3.4 Burst forwarding network data scheduling

The burst forwarding network scheduling function mainly serves two purposes, on demand vertical channel creation and data forwarding over virtual channel. This section describes these two procedures in detail. A typical data forwarding process is presented, which includes the virtual channel creation, data forwarding and virtual channel tear down.

As shown in **Figure 79**, 5 data sources access with 10Gbps link sends data to a 40Gbps link. The egress port maintains a table which records the accumulated bandwidth allocated for the virtual channels. Assumes that there is no virtual channel allocated in the egress port at the beginning. When burst 1 data transmission starts, the network create a virtual channel for the burst transmission. The egress port checks the port rate filed of the header burstlet. It allocates 10Gbps resource for the burst. Same procedure for burst 2, burst 3 and burst 4. At this point, the 40Gbps link is virtually divided into four 10Gbps links. When the fifth burst arrives, the data transmission is blocked since the egress port cannot provide more bandwidth. The data transmission of burst 5 can only start when one of the previous 4 data transmission finishes.

The burst forwarding router maintain the burst transmission speed. Since all data sources access the network with the same speed (10Gbps), the scheduler use round robin to forward each burstlet. In the 40Gbps link, it seems like the burstlets from the four burst are interleaved, but the forwarding speed of each burst maintained at 10Gbps. In the ingress port side, the burstlets are identified and categorized into different burstlet buffer using the burst ID. The burst ID management mechanism is described in the following part of this section.

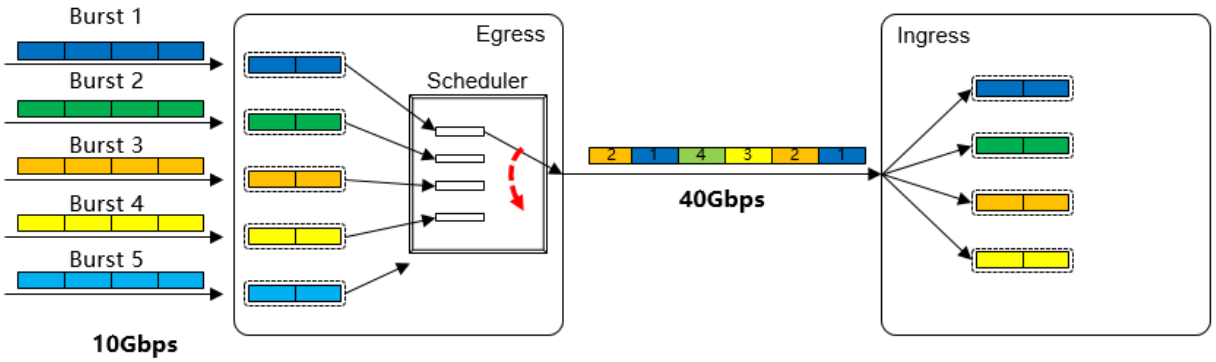


Figure 79- Burst scheduling mechanism

Figure 80 depicts the detailed virtual channel creation process. A virtual channel is created on demand for one specific burst transmission. In the first step, once the head burstlet is received, the router firstly select the egress port based on the routing information carried in the head burstlet. Based on the selected port, the router starts to allocate the bandwidth required for the specific burst transmission. As shown in the second step, each egress port maintains an ID resource list which records the previously allocated virtual channel. The ID number corresponds to the available bandwidth of the physical port. Each ID represent the greatest common divisor of the bandwidth in the network, e.g., FE port. Based on the **port rate filed** carried in the head burstlet, one burst virtual channel might require multiple IDs in the port. As shown in **Figure 80**, port 4 is selected as the egress port. Based on the head burstlet information, only one ID is required. By checking the ID resource list of P4, ID 3 is available. In the third step, ID 3 is marked as "occupied" in the ID resource list indicating this ID is allocated for the virtual channel being created. If the ID resource list is fully occupied, the burst forwarding is blocked. It is resumed once the ID is released by other burst transmission. Once the ID is allocated, as shown in step 4, an entry is added in the forwarding table. The following body burstlets and tail burstlet will be forwarded according to the records in the forwarding table.

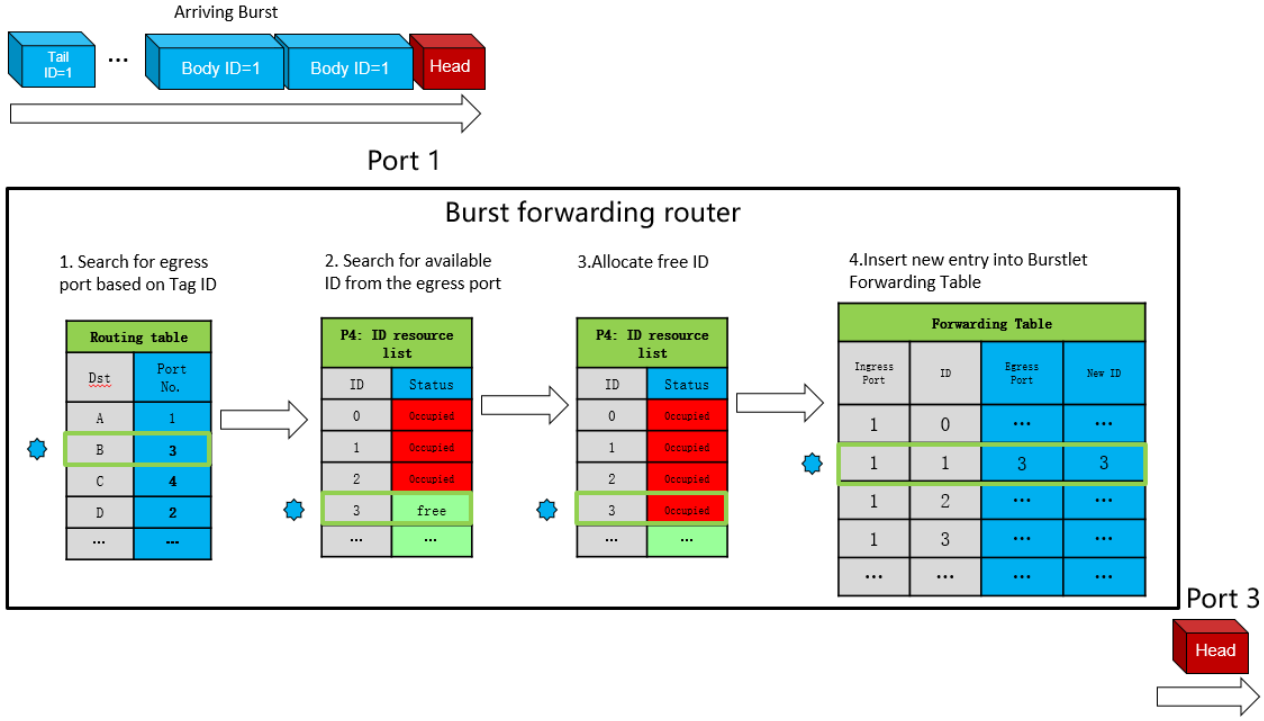


Figure 80- Virtual channel allocation process

The burstlet forwarding table is a port based local forwarding table. It is created by the head burstlet, and used by the body and tail burstlet for data forwarding. As shown in the burst forwarding table of

Figure 81, the burstlet with ID 1 received from port 1 is forwarded to egress port 3 with a new ID 3. The value of NewID is unique per port at a time, it is a mechanism to guarantee that different outgoing bursts from the same egress port have different burst ID. For example, if both ingress port 1 and ingress port 2 receives bursts with same ID and they are heading to the same egress port 3. Assumes that the port rate of port 3 is higher than port 1 plus port 2, two virtual channels are established and the burstlet from port 1 and port 2 are interleaved. However, if the outgoing burst ID is not changed, it is impossible for the router in the next hop to identify the body and tail burstlet of these two bursts.

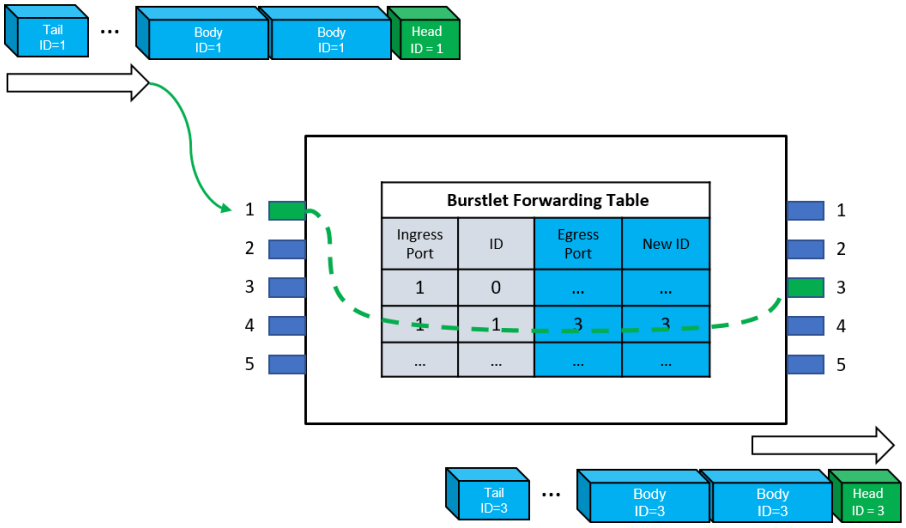


Figure 81- Burstlet forwarding procedure

The virtual channel in the burst forwarding router is destroyed after the complete burst has been forwarded. As shown in **Figure 82**, when the tail burstlet is received by the router, the egress port is checked in the ID forwarding table. In the second step, the previously allocated ID in the resource list is released. Finally, in step 3, the forwarding table entry is removed after the tail burstlet forwarding.

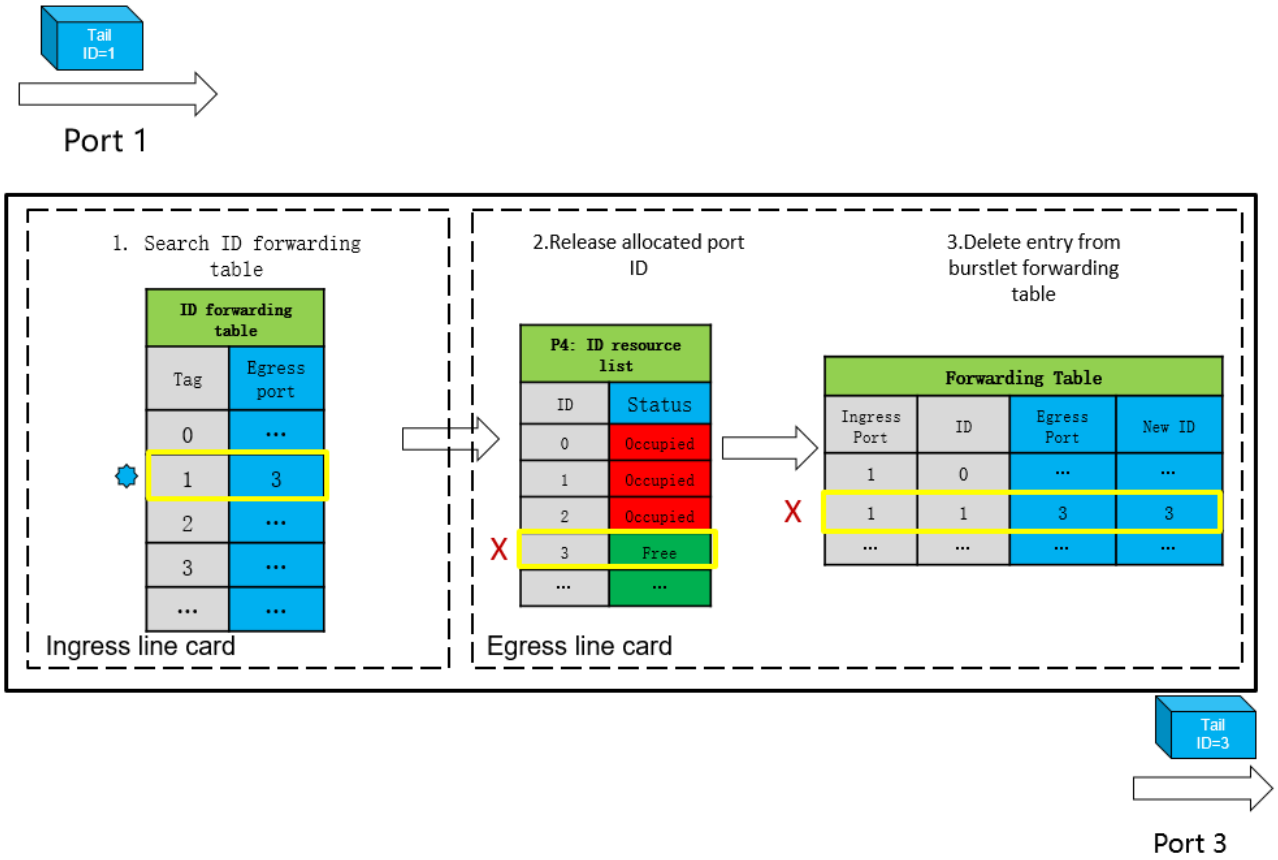


Figure 82- Virtual channel tear down procedure

15.3.5 Host side design

The burst forwarding network requires the end host to send each burst using NIC line rate. However, the current socket interface only support sending data as a stream (TCP) or as a datagram (UDP). TCP is used by most of the application because of the reliable transmission and self-tuning transmission rate control. Other popular transport protocol, e.g., QUIC, is built on top of UDP. The flow management, reliability and security features are developed in the user space. Both TCP and QUIC send application data as data stream. As shown in **Figure 83**, the end host OS that supports burst forwarding should provide a new socket function. The new socket interface should support the burst sending at NIC line rate. The transmission speed should not be limited by any flow control algorithm.

However, sending uncoordinated burst to the network is dangerous. It can easily create network congestion and packet loss. The burst forwarding host first ask for the transmission permission. Once the transmission is granted, the burst can be transmitted. Instead of implementing self-maintained congestion control algorithm, the burst forwarding host cooperates with the flow control function of the network to ensure congestion free. The burst forwarding host keeps monitoring the received traffic information. If the received data is too much to handle by the host, a back pressure message should be issued to the application and block the burst transmission.

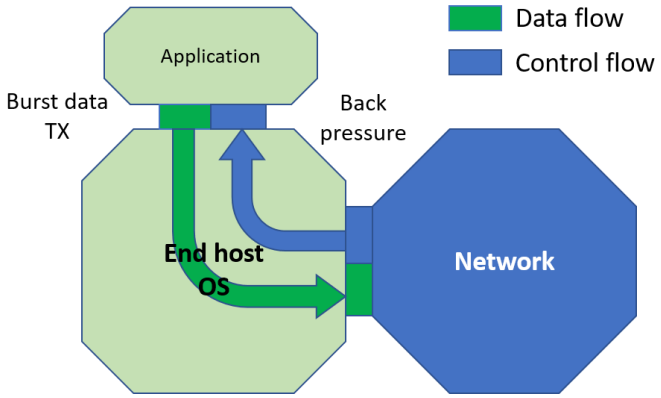
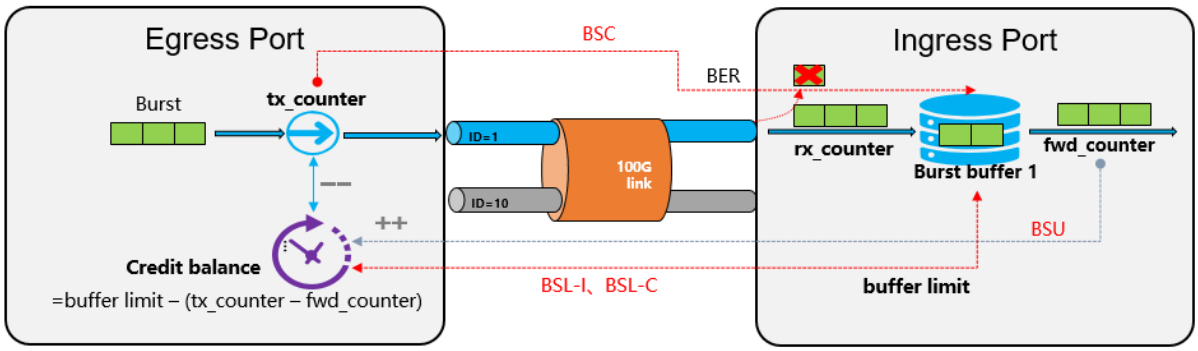


Figure 83- Burst forwarding host data transmission and flow control interface

15.3.6 Flow control functions

The flow control function of the burst forwarding network mainly serves two purposes, to ensure the network congestion free and to arrange the burst transmission in sequence. The burst forwarding network does not bind with any specific flow control functions. If the burst forwarding router has very shallow buffer or the application requires extremely low end to end latency, global TDMA-like scheduling can be utilized. However, such method could sacrifice the bandwidth which depends on the network scale and time synchronization accuracy. Another possible approach could be based on transmission token. Only the data sources with the token can start the burst transmission. The total number of token depends on the egress port bandwidth. However, this method usually works best in the application with aggregation tree topology where the message destination is centralized, e.g., cloud access service.

If the burst forwarding network can tolerate some buffer usage, the Quantum Flow Control (QFC) mechanism can be utilized. Different from traditional host based congestion control algorithm, QFC is a distributed port based credit flow control algorithm. By using QFC, the amount of packet that can be sent from the egress port to the next hop ingress port is explicitly calculated. In order to accommodate burst forwarding, the algorithm is updated to support virtual channel creation.



BSU: buffer state update; **BSC**: buffer state check;
BSL-I: buffer state limit indicate; **BSL-C**: buffer state limit confirmation;

Figure 84- QFC flow control algorithm for burst forwarding network

The burst forwarding QFC mechanism is described in **Figure 84**. The ID marked in the connection link is the created virtual channel ID. In the ingress port side, a burst buffer is allocated for each virtual channel. During the initialization phase, the capacity of the burst buffer of the ingress port is sent to the egress port via BSL-I message. This message is confirmed by the BSL-C message. During the run time, the burst buffer utilization can be calculated by subtracting fwd_counter from rx_counter value. In order to avoid buffer overflow, the ingress port keeps posting the fwd_counter value using the BSU message to the egress port device. On receiving the BSU message, the egress port device calculates the available buffer of the

ingress port using $\text{BufferLimit} - (TxCounter - FwdCounter)$. The result is called credit balance. Meanwhile, the egress port periodically sends the BSC message to correct the possible mismatch between tx_counter and rx_counter due to packet transmission error. Since the egress port only sends data which can be stored in the ingress port buffer, the link is lossless from buffer overflow.

15.4 Conclusion

This document describes the burst forwarding technology, an application oriented data forwarding mechanism. A burst is a basic application process unit. The size of the burst depends on the application type. The burst forwarding host sends the burst using line rate of the NIC. The burst forwarding network forwards the burst with the same speed as it is injected into the network. If the concurrent data transmission excess the network capacity, the extra transmission is blocked until the previous burst transmission finishes. Since the entire burst is forward by the network from the data source to the destination, the averaged application data transmission time is much shorter. The application in the destination node can immediately start processing the data once the burst is received, thus the utilization efficiency of the compute resource is optimized.

16 Network Slicing Architecture

16.1 Introduction

Network slicing, despite not being a new concept [NS-1, NS-2, NS-3], acts as a foundational concept and systems to current 5G/future networks and service delivery, with the goal of providing dedicated private networks tailored to the needs of different verticals based on the specific requirements of a diversity of new services such as high definition (HD) video, virtual reality (VR), V2X applications, and high-precision services [NS-30].

Network Slicing (NS) is an end-to-end concept [NS-4, NS-5] covering all network and cloud network segments (access, core, transport, edge). It enables the concurrent deployment of multiple logical, self-contained and independent shared or partitioned network resources and a group of network and service functions on a common infrastructure platform.

Network Slice can be defined [NS-7] as a set of infrastructures (network, cloud, data center) components/network functions, infrastructure resources (i.e., connectivity, compute, and storage manageable resources) and service functions that have attributes specifically designed to meet the needs of an industry vertical or a service. As such a Network Slice is a managed group of subsets of resources, network functions/network virtual functions at the data, control, management/orchestration, and service planes at any given time. The behavior of the Network Slice is realized via network slice instances (i.e., activated slices, dynamically and non-disruptively re-provisioned). Network Slices considerably transform the networking perspective by abstracting, isolating, orchestrating, softwarizing, and separating logical network components from the underlying physical network resources and as such they are inter-twined to enhance Internet architecture principles.

In the foreseeable future (e.g., 2030), different forms and factors of network slicing are expected to become the norm, realized through diverse operational modes and taking multi-tenancy and precision slicing to an extreme. As such, slicing impact is broad in terms of networking (i.e. feature-, capability-rich and value-rich) and deep from both a vertical (multi-layer) perspective as well as a horizontal (end-to-end and multi-domain) view. A future-thinking perspective on cloud network slicing takes customer/tenant-provider recursive relations to an extreme combined with flexible tenant-driven choices on the network protocol stack and actual software instances under its responsibility.

In this chapter, we provide a multi-faceted overview of network slicing efforts, starting with a primer on the topic from multiple perspectives, and presenting a future looking view on 2030 Network Slicing characteristics, enablements, and open challenges upfront.

16.2 Network Slicing Primer

Slicing is a move towards on demand segmentation of resources and deployment of virtual elements for the purpose of enhanced services and applications on a shared infrastructure. Therefore, slicing should be considered from multiple viewpoints, technical and business ones. Many groups including ITU-T, ETSI, IETF, 3GPP, ONF in addition to open source and research projects are currently considering slicing as a tenet of their assets.

In this section, we present key characteristics and viewpoints around slicing and provide a short survey of the state of the play in the evolving work on network slicing and identification of key intellectual contributions from different initiatives at various timelines.**11.2.1 Slicing viewpoints**

Network Slicing is a management mechanism that a resource provider can use to allocate dedicated partition infrastructure resources and service functions to users. Broadly, partition strategies can be classified into three categories:

- Physical separation, such as dedicated backbones or dedicated data centers. However, this strategy is not cost efficient.
- Underlays/overlays supporting all services equally (‘best effort” support), such as underlays / overlays, in the form of VPN as overlay solution. These solutions are neither flexible nor agile.
- Slicing, through cloud network resources allocation, where dedicated resources per customer/service ensure both isolation and customization on top of the same infrastructure.

Within the context of provisioning of slices, there are three key roles that a participant in the slicing arena can undertake. These roles are the following:

- *Resource Provider:* A resource provider owns the physical resources and infrastructure, in any of network/cloud/datacenter, and provides or leases them to operators who wish to be slice providers. The resource is presented as slice parts, which can be composed together to form a full slice.
- *Slice Provider:* A slice provider is the organization from which NS can be procured and created. They are typically a telecommunication operator but could be any organization that can participate in the slicing market.
- *Slice Tenant:* A slice tenant is the owner of a specific slice, in which customized ser- vices are hosted. Slice tenants make requests for the creation of new slices, from a slice provider, through a service slice model specification. The tenant runs their services in the slice on behalf of their users.

For any role, an organization can take a viewpoint on sharing and partitioning of resources.

From a business point of view, a network slice includes a combination of all the relevant network and compute resources, functions, and assets required to fulfill a specific business case or service.

From the infrastructure point of view, Network slice instances require the partitioning and assignment of a set of resources that can be used in an isolated, disjunctive or non- disjunctive manner for that slice.

From the tenant point of view, Network slice instance provides different capabilities, specifically in terms of their management and control capabilities, and how much of them the network service provider hands over to the slice tenant. As such, there are two types of slices:

- *Internal slices*, understood as the partitions used for internal services of the provider, retaining full control and management of them.
- *External slices*, being those partitions hosting customer services, appearing to the customer as dedicated networks/clouds/data centers.

From the management plane point of view, Network slices refer to the managed fully functional dynamically created partitions of physical and/or virtual network resources, network physical/virtual and service functions that can act as an independent instance of a connectivity network and/or as a network cloud. Infrastructure resources include connectivity, compute, and storage resources.

From the date plane point of view, Network slices refer to dynamically created partitions of network forwarding devices with guarantees for KPIs, isolation, customization and security.

16.2.2 Key Characteristics

Slices are expected to considerably transform the networking perspective by

- Abstracting away the lower level elements, in various ways.
- Isolating connectivity at a sub-network level.
- Separating logical network behaviors from the underlying physical network resources.
- Allowing dynamic management of network resources by managing resource-relevant slice configuration.
- Simplifying and automating of operations.
- Support for rapid service provisioning.
- Support for NFV deployment.

Key characteristics of the Network Slicing include:

- The *concurrent deployment* of multiple logical, self-contained and independent, shared or partitioned slices on a common infrastructure platform.
- *Dynamic multi-service support, multi-tenancy* and the integration means for vertical market players.
- The *separation of functions*, simplifying the provisioning of services, the manageability of networks, and integration and operational challenges especially for supporting communication services.
- The means for Network /Cloud operators/ ISP and infrastructure owners to *reduce operations expenditure, allowing programmability and innovation* necessary to enrich the offered services, for providing tailored services, and allowing network programmability to OTT providers and other market players without changing the physical infrastructure.
- *Hosting applications*, offering the capability of hosting virtualized versions of network functions or applications, including the activation of the necessary monitoring information for those functions.
- *Hosting on-demand 3rd parties*/OTTs, empowering partners (3rd parties / OTTs) to directly make offers to the end customers augmenting operator network or other value creation capabilities.
- Additional characteristics, requirements, use cases, standard and research activities on Infrastructure slicing and references are presented in the tutorial [NS-8]

16.2.3 KPIs Slicing

SDOs and community fora like ETSI NFV Industry Specifications Group, 3GPP, and others have been concerned with the definition of KPIs for slicing, which are classified into the following categories:

Accessibility KPIs: [NS-9] Give a figure of how well the resources provided through slices are accessible. Specific KPIs are how many customers are registered to a given slice as well as the ratio between the number of successful registries and the total number of registration requests.

Integrity KPIs: [NS-9] Integrity is related to the capability of the network slice to deliver information end to end. The specific KPIs consist of the end-to-end delay and the throughputs that can be achieved in a slice instance between particular reference points of 5G networks.

Utilization KPIs: [NS-9] These KPIs represent how much used are the resources of a slice. Specifically, these KPIs are the mean number of sessions that are successfully established per slice and the usage of the virtualized resources, i.e. virtual processor, virtual memory, and virtual disk, in the slice.

Additional classification of network slicing KPIs [NS-10] are :

Slice runtime and slice life cycle management related. For slice runtime, this work considers three types of resources that may be used by a single slice, namely connectivity, computing, and memory. For each type of resources, it defines two thresholds, namely underutilization threshold and overutilization threshold. The underutilization threshold is an arbitrary percent of the capacity of a given type of resource. For example, the underutilization threshold for connectivity could be set to 20% and that means that if the bandwidth of a particular virtual link that is being used during a given observation time window is little or equal than the 20% of the capacity of that link, then the link is marked as underutilized. In a similar way, the overutilization threshold is defined. As there are three different types of resources that are consumed by a slice and two thresholds for each, with a total of six KPIs come out. Six more KPIs are defined that can complement the behavior of the management system in charge of allocation of resources.

Slice life cycle management related KPIs [NS-10] includes a total of four additional KPIs, namely the slice deployment time, slice deployment time scalability, reconfiguration execution time, and slice termination time. Indeed, all these four KPIs are related to every single slice.

16.3 Analysis of Network Slicing Landscape

Slicing itself is not new, it has been considered in the past and it is progressively being included in the 5G standards, as discussed in this section.

The followings are early definitions, technologies, and intellectual roots of slicing:

i) Active / Programmable Networks research: In the hindsight, the ability to define, deploy and operate user-defined network instances in isolation through the node operating systems and resource control frameworks part of Programmable Networks for IP Service Deployment [NS-1] can be seen as early forms of network slicing (1995 -2005).

ii) Federated Research Testbeds: Likewise, the notion of users (experimenters) requesting and having allocated computing and networking resources over shared and federated infrastructures providing certain levels of functional and performance isolation can be also regarded as initial slicing approaches. Remarkable examples include Planet Lab USA (2002), PlanetLab EU (2005), OneLab EU (2007), PlanetLab Japan (2005), OpenLab EU (2012).

iii) GENI Slice (2008-): GENI [NDS-11] is a shared network testbed, where multiple experimenters are able to run different experiments based on a custom set of resources at the same time. According to GENI, a slice is: i) The unit of isolation for experiments; ii) A container for resources that are used in an experiment. GENI experimenters add GENI resources (compute resources, network links, etc..) to slices, and run experiments that use these resources; iii) A unit of access control. The experimenter that creates a slice can determine which project members have access to the slice, i.e., are members of the slice.

iv) Slice capabilities (2009) Management and Service-aware Networking Architectures (MANA) identified 3 Slices capabilities [NS-2] : "Resource allocation to virtual infrastructures or slices of virtual infrastructure."; "Dynamic creation and management of virtual infrastructures/slices of virtual infrastructure across diverse resources."; "Dynamic mapping and deployment of a service on a virtual infrastructure/slices of virtual infrastructure."; ii) 17 Orchestration capabilities; iii) 19 Self-functionality mechanisms; and iv) 14 Self-functionality infrastructure capabilities.

v) Cloud manifest (2009) as defined in the RESERVOIR federated cloud environment [SC3], the cloud manifest specifies the structure of the service application in terms of component types that are to be deployed as virtual elements. The manifest also specifies the grouping of components into virtual networks and tiers that form the service applications, i.e., yet another shape of the network slicing concept.

Standards Development Organizations (SDOs) and some other industrial associations are looking at the network slice concept from different angles and perspectives with small differences which may trigger incompatibilities among the different approaches.

The followings are SDOs initiatives on Network Slicing:

vi) ITU-T Slicing (2011). As defined in [NS-12], **Logically Isolated Network Partitions (LINP)** considers a slice as a unit of programmable resources such as network, computation, and storage, i.e., the basic underpinnings of the Network Softwarization concept that emerged in early 2010s.

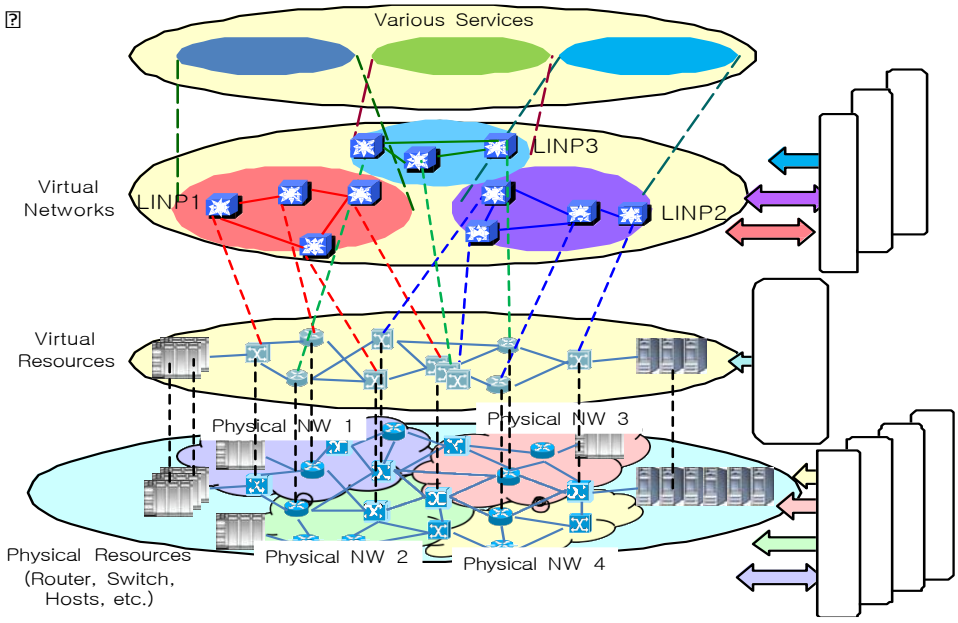


Figure 85- Conceptual architecture of ITU-T Logically Isolated Network Partitions.

vii) ITU-T IMT2010/ SG13 (2018/2019) - More recently**,** [NS-13, NS14] describes the concept of network slicing and use cases of when a single user equipment (UE) simultaneously attaches to multiple network slices in the IMT-2020 network. The use cases introduce the slice service type to indicate a specific network slice and the slice user group for precisely representing the network slice in terms of performance aspects and business aspects. This Recommendation also specifies high-level requirements and framework for the support of network slicing in the IMT-2020 network, as illustrated in **Figure 86**.

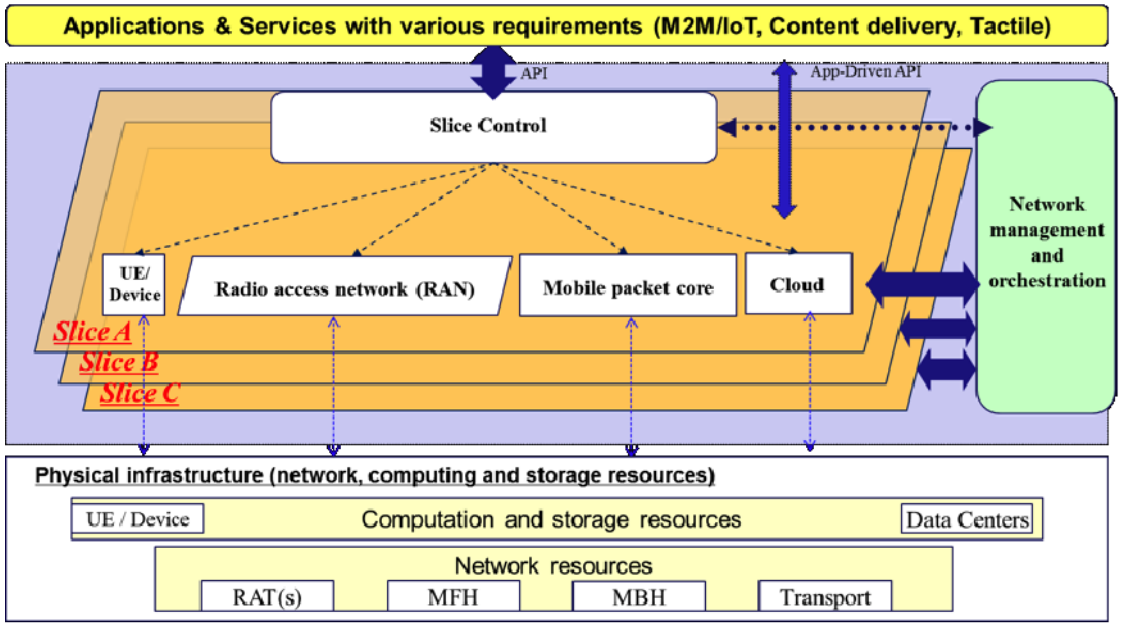


Figure 86- ITU-T IMT2020 Slicing Representation

viii) IETF (2017) Network Slicing is defined in [NS-7] as managed partitions of physical and/or virtual network and computation resources, network physical/virtual and service functions that can act as an independent instance of a connectivity network and/or as a network cloud. Network resources include connectivity, compute, and storage resources. As such Network Slices considerably transform the networking and servicing perspectives by abstracting, isolating, orchestrating, softwarising, and separating logical network components from the underlying physical network resources and as such they enhance Internet architecture principles. The IETF Network Slicing (acronym netslicing) work group [https://datatracker.ietf.org/wg/netslicing/about/] in the Operations and Management (ops) area concluded its tasks in 2019, and the respective draft documents and presentations can be found at the web: [https://datatracker.ietf.org/meeting/99/session/netslicing]

ix) 3GPP Started the studies on "Network Slicing' in 2016 [NS-15]. Relevant technical reports (TR) and technical specifications (TS) on Network Slicing is included in [NS-16]. This study is valid for both 4G and 5G systems. Two other studies are presented in [NS-17]- Study on tenancy concept in 5G networks and network slicing management, and in [NS-18] - Network slice management enhancement. The current Network Slicing architecture is defined in the following Technical Specifications:

- [NS-19] Charging management; Network slice performance and analytics charging in the 5G System (5GS);
- [NS-20] Charging management; Network slice management charging in the 5G System (5GS).

x) GSMA The GSMA Association (GSMA) is active in forming guidelines for the mobile communications ecosystem in terms of common network slices. The GSMA sets out to understand the service requirements expressed by business customers from different vertical industries in several key sectors, including energy, IoT, automotive, manufacturing and many more. Further to that, the GSMA working with operators and vendors have defined a Generic Slice Template (GST) to facilitate operators to sign a Service Level Agreement (SLA) with verticals and enable interoperability and roaming. The related working groups of the GSMA are NEST and North America NETSLIC. The NEST working at the global level to define the GST and a respective attribute

(such as bit rate, latency, reliability, etc.), and their value ranges. The GST is presented in the GSMA PRD NG.116, which is a formal Permanent Reference Document to provide guidelines for the interoperating mobile network operators to set up a common set of the Network Slices. The aim of the task is to ensure interoperability and to enhance the user experiences cross the ecosystem. The North America NETSLIC Task Force focuses on the region, and its focus is on complementing the work of the global NEST. More specifically, the NETSLIC interprets, assesses and prioritizes the documentation of the regional needs of the verticals in a form of additional GST information as an input to the GSMA PRD NG.116. In addition to these main groups of the GSMA dealing with Network Slicing, there also are subgroups that discuss and contribute to these main working groups of Network Slicing of the GSMA, such as the Next Generation Vertical Task Force (NGVT) of the global level, and the North Americas Vertical Applications working group (NAVA).

xi) NGMN (2016) The Next Generation Mobile Networks (NGMN) Alliance view on slicing considers of 3 layers: 1) Service Instance Layer, 2) Network Slice Instance Layer, and 3) Resource layer. The Service Instance Layer represents the services (end-user service or business services), which are to be supported. Each service is represented by a Service Instance. Typically, services can be provided by the network operator or by 3rd parties. A Network Slice Instance provides the network characteristics, which are required by a Service Instance. A Network Slice Instance may also be shared across multiple Service Instances provided by the network operator. The Network Slice Instance may be composed by none, one or more Sub-network Instances, which may be shared by another Network Slice Instance. The high-level concept of network slicing and definitions in presented in [NS-21]. The NGMN 5G vision and outlook identifies a rich set of requirements grouped along the six dimensions of user, system, device, service enhancement, network management and business requirements.

xii) ETSI E2E Network Slicing [NS-23] identifies a next-gen network slicing (NGNS) framework defined here as a generalized architecture that would allow different network service providers to coordinate and concurrently operate different services as active NS, including slicing design principle (service-oriented approach, slice abstraction, slice reusability, slice autonomy), an information model, network slice function specification, and slice enablement. ETSI NFV specifies network operators' perspectives on NFV priorities for 5G, network slicing support with ETSI NFV architecture and an E2E network slicing framework.5G resource management and orchestration aspects were added on top of the NFV Release 2 architecture framework. As a result, new NFV Release 3 features that closely relate to 5G include: "Support for network slicing in NFV", "Management over multi-administrative domains", and "Multi-site network connectivity". These features are essential to address the variety of applications expected to run on top of a 5G system, whether using distributed resources over multiple sites, centralized or a combination of both. Another recent development within ETSI Zero Touch Network and Service Management Industry Specification Group (ZSM ISG) is specifically devoted to the standardization of automation technology for network slice management [NS-25]. Within the ETSI Multi-access Edge Computing (MEC) group, a new work item called "MEC support for network slicing" [NS-24] seeks to identify the necessary support for network slicing, evaluating the gaps from MEC features and functions, and identify the new requirements.

xiii) ONF identifies how to apply SDN to network slicing. The Open Networking Foundation (ONF) has issued "Applying SDN Architecture to 5G Slicing" [NS-26]. The ONF SDN architecture defined in [NS-27] is based on providing a complete view of all resources required to serve a business purpose, which matches key principles of Slicing in a network. As a conceptual framework for a standardized platform supporting Network Slicing, it can serve as one of the technical building blocks to fulfil the business requirements for the fifth generation of mobile technology.

xiv) BBF Broadband Forum [NS-28] is also approaching network slicing (BBF, 2018) by augmenting the previous management functions by defining new and complementary ones, like Access Network Slice Management (ANSM), Core Network Slice Management (CNSM), and Transport Network Slice Management (TNSM). Each of them is intended to take care of the slice lifecycle management of each particular network slice subinstance (i.e., access, core, or transport).

xv) MEF Metro Ethernet Forum produces specifications related to Network Slicing. An example is the MEF specification for SD-WAN [NS-29]

16.4. Network 2030 Slicing

A number of key capabilities for network slicing are envisaged for Network 2030 and they are presented in this section and **Figure 87**.

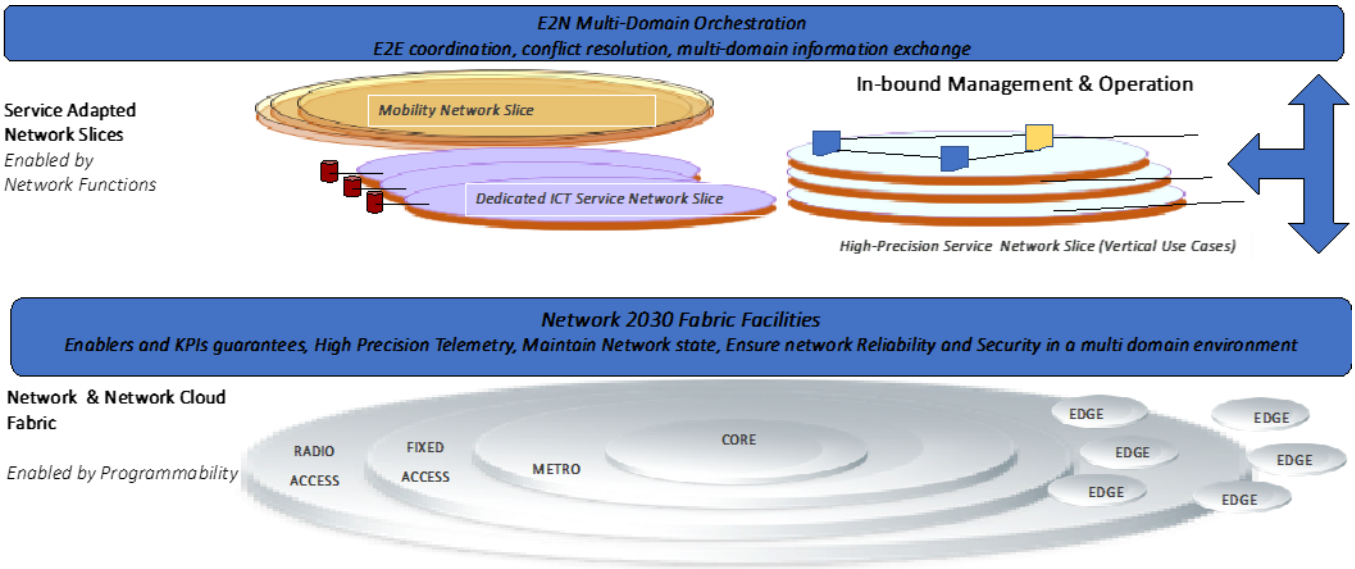


Figure 87– Network 2030 Slicing Characteristics

The key challenges from a provider's perspective on (i) scalability, (ii) arbitration, (iii) slice planning and dimensioning, and (iv) multi-domain. From the business side, some key implications include: (i) coordination models, (ii) inter-provider SLAs, (iii) pricing schemes, (iv) service specification, and (v) customer-facing advertisement. From a technical perspective, implications worth to be highlighted: (i) slice decomposition, (ii) discovery of domains, (iii) common abstraction models, (iv) standard interfaces, protocols, and APIs, (v) high precision telemetry,

Key concepts calling for action when jointly applying slicing to cloud and network resources in multiple technical and administrative domains are provided below:

- A (cloud) network slice supports at least one type of service.
- A (cloud) network slice may consist of cross-domain components from separate domains in the same or different administrations, or components applicable to the infrastructure.
- A resource-only partition is one of the components of a (Cloud) Network Slice, however on its own does not fully represent a Network Slice.
- A collection of slice parts from separate domains is combined, connected through network slices, and finally aggregated to form an end-to-end cloud network slice.
- Underlays / overlays supporting all services equally (with 'best effort" support) are not fully representing a Network Slice.

The followings are *precision network slicing challenges* as applicable to NETWORK 2030:

- Slice Templates and Methods for the design of slices to different scenarios in Vertical market players (such as the automotive industry, energy industry, healthcare industry, media and entertainment industry, holograms, etc.). This outlines an appropriate slice template definition that may include capability exposure of managed partitions of network resources (i.e. connectivity compute and storage resources), physical and/or virtual network and service functions that can act as an independent connectivity network and/or as a network cloud.

- Interaction with the vertical tenants: Proper abstractions and templates must be defined for ensuring the provision of a consistent service portfolio and their integration with the internal network management and orchestration of vertical tenants.
- Network Slicing Service Mapping - service mapping model binding across network slicing; methods to realize diverse service requirements without re-engineering the infrastructure.
- High level of recursion, namely methods for network slicing segmentation allowing a slicing hierarchy with parent–child relationships.
- Native programmability and control of Network Slices - Capability exposure for Network Slicing (allowing openness) with APIs for dynamic slice management and interaction.
- Precision Slicing - concurrent deployment of multiple logical, self-contained and independent, shared or partitioned networks on a common infrastructure with guaranties for KPIs (Key Performance Indicators)
- Guaranteed Isolation - slice creation and deployment with guarantees for isolation in each of the Data / Control / Management / Service planes. Methods to enable diverse requirements for slicing, including guarantees for the end-to-end QoS of a service within a slice.
- High Scalability characteristics - In order to partition network resources in a scalable manner, it is required to clearly define to what extent slice customers can be accommodated or not on a given slice. The application of different SLAs on the offered capabilities of management, control and customization of slices will directly impact the scalability issue.
- Autonomic slice management and operation, namely self-configuration, self-composition, self-monitoring, self-optimization, self-elasticity for slices that will be supported as part of the slice protocols.
- Customized security mechanisms per slice - In any shared infrastructure, security is a key element to guarantee proper operation, and especially a fair share of resources to each user including Resource isolation and allocation policy at different levels and Isolation of network service management for multiple tenants.

17 Network Management

17.1 Introduction

A high level Network2030 architecture and basic requirements are described in Section 9.2. Section 17 describes additional Network2030 management requirements, management functional areas, the intent management framework, the autonomic characteristics, the AI/ML role in management and orchestration for Network 2030.

17.2 New Approaches to Management

Another challenge will involve enabling operators and users to manage Network 2030 infrastructure and services including software-defined networks at scale. This will require further automation and the closing of management control loops. In the past, where possible and where routine tasks are involved, human operators have been increasingly taken out of the loop and replaced with management systems and controllers that were in most cases hosted in a central location or in the cloud. The ever-increasing need for shorter control loops means that management services will increasingly need to migrate closer to the edge of the network and indeed into devices themselves.

However, despite all those advances, networks will not become clairvoyant and need to be given guidance for certain tasks and require some degree of human interaction. For this reason, advances in abstractions will be required to facilitate the ways in which operators can interact with networks. These abstractions are needed for productivity reasons (operate at greater scale) and to constrain complexity (greater heterogeneity, growing number of interdependencies which are becoming less understood, etc.).

Technologies such as Intent-Based Networking, which will allow networks to be managed by defining outcomes rather than prescribing rules or procedures, are expected to provide significant contributions here. While vendors frequently tout their controller interfaces and policy frameworks as "intent interfaces", true intent technology is still in its infancy. For example, intent technology will require novel human/machine interfaces that allow to iteratively infer and refine intent. It will also require advances in the application of AI and Machine Learning technology that are able to automatically define and continuously refine plans of actions that generate desired outcomes.

Furthermore, in order to meet scalability challenges, novel management architectures may need to be supported that support greater management functionality in distributed or decentralized manner across the network, as opposed to relying solely on centralized management systems and controllers as predominantly the case today.

17.3 Assuring QoS via Resilience

In Network 2030 we envision new and networked applications – such as remote surgery, and multi-party holographic communications – that will demand extremely fast resource management. At the same time, the network will increasingly have to be treated as a critical infrastructure that needs to offer an uninterrupted service. The network and the services that run on it – supporting these new and demanding applications – will demand autonomic management, i.e. management that contains closed management loops operating at very fast timescales. Autonomic management will not necessarily be required for all services or even for all parts of the (highly interconnected) network. There will be applications for which "best effort" will always be appropriate – and in such cases there is no need to devote extra resources to ensuring their Quality of Service (QoS). Also, there will always continue to be aspects of management – for example for longer-term resource planning and deployment – for which closed /fast loops are not necessary; in these situations, a human expert or team will be closing the loop

[NM.4].

A great deal of prior work has been on network and service management, not least within ITU standardization, so in this document and section we focus on new and future requirements and on mechanisms that will be needed for the Network 2030 context. Support for QoS assurance via management is a vital and integral part of what follows.

In this section we focus on – and emphasize the need for – a new approach, namely resilience management, which is currently or not typically offered in network management solutions. In this section, we first outline what is meant by resilience, then provide a brief rationale for its adoption, and finally we describe a framework in which structural and operational resilience can be realized. The traditional "FCAPS" approach to network management urgently needs to be modernized to become "RCAPS", where Resilience (R) replaces Fault (F) because networks (as critical infrastructures in the modern world) are subject to many more sources and sorts of challenges than simply faults.

Resilience is the ability of a network or system to provide and maintain an acceptable level of service in the face of any failure or challenge to normal operations (e.g. a natural disaster or a cyber-attack). At the network (topology) level, resilience amounts to preserving throughput, loss, jitter, and latency as successfully as possible for a given service — all these Quality of Service (QoS) aspects can be compromised if failures/attacks occur, and especially if there is a lack of resilience mechanisms to remediate/mitigate them. At the service level, the important aspects that need to be maintained include, most importantly, service availability and service reliability [NM.6].

Resilience takes on additional importance for future networked services, because in many cases these services are used for mission-critical applications and require high precision, and certainly moving beyond the "best effort" that was acceptable for the support of many applications in the past.

- Future networked services will be characterized by the need for highly precise timing (e.g. in- time and on-time services) and synchronization between large numbers of flows (coordinated services). Any degradation puts these services in jeopardy and makes the applications that rely on them infeasible.
- Where degradations are acceptable, the mechanisms and extent of degradation need to be controlled more precisely than today (e.g. qualitative services). Hence there will be much higher demands on resilience (and how resilience is integrated into the network service).

The ultra-low-latency requirements, and the huge increase of bandwidth demands of future networked services such as holographic type communication services and vehicle-to-vehicle communications, make an unrecovered failure a significant loss for network operators. Therefore, network resilience is of paramount importance to maintain the network QoS and high availability and reliability of these new and extremely demanding services. The assurance of QoS has a fairly long history (notably [NM.1] [NM.9]), but it deserves renewed attention in Network 2030, and this is particularly relevant and important because of the symbiotic relationship between QoS and resilience in the context of autonomic network management, as outlined in this document.

The definition of network resilience subsumes several related disciplines that aim to address faults and challenges. Sterbenz et al. [NM.8] have defined an organization of these disciplines, which places them into two categories: i) those related to *challenge tolerance*, which address the design and engineering of resilient networks; and ii) *trustworthiness* disciplines that provide ways to describe the resilience of a networked system.

There are many methods for designing network resilience. The first is to provide redundancy and diversity of logical and physical entities. Logical entities can include network paths as well as functional entities such as policing, classification, and scheduling. Physical entities include ports, routers, and router line cards. The second is to use protocols to provide quick re- convergence and to maintain high availability of existing connections after a failure event occurs in the network. Among the other techniques is the use of packet replication or network coding to overcome packet loss, and also error correction techniques.

Although redundancy and diversity enable high availability and reliability, they impose higher costs for realization of the network service. In order to keep such costs at an acceptable level, the addition of redundant instances must be driven by the target resilience, keeping in mind cost limitations that apply to a network service implementation. Also, applying redundancy and diversity might impose additional complexity of managing the redundant instances and updating their states in order to keep them ready for taking over the functionality of faulty instances.

Service Level Agreements (SLAs) for future networks will be expected to cover appropriate resilience objectives of availability and reliability as well as QoS specifications in terms of required performance (throughput, latency, and jitter); these will all need to be monitored and controlled by the management system. This statement of intent will be mapped into the appropriate resilience and QoS measures and mechanisms to avoid violating the SLA. Since network or application/service failures can also be caused by cyber security attacks, the network operator needs to apply relevant security policies and provide necessary tools to detect and mitigate these attacks, or to prevent them.

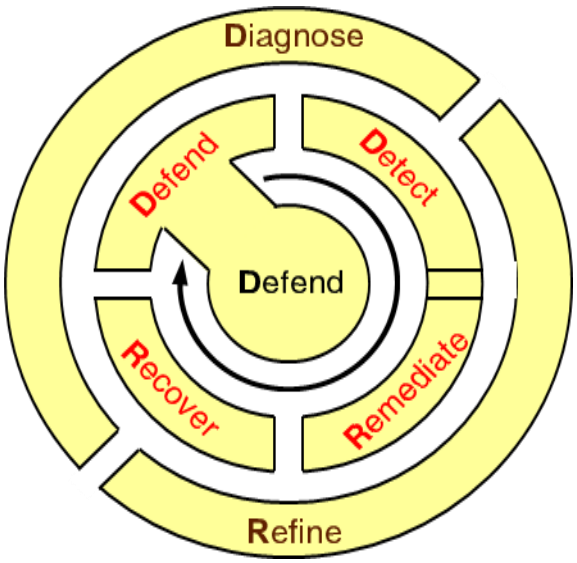


Figure 88–Closed loop resilience management strategy

To design, build, or adapt networked systems to be resilient, we may use the D^2R^2+DR strategy, which is essentially two sets of steps organized in two 'loops' as shown in **Figure 88**. The inner loop, D^2R^2, is intended to operate in real time (or as fast as possible) in order to detect and correct anomalies, whereas the outer loop, DR, can act more sedately (initially offline, mediated by a human expert, but ideally in the future it will function autonomously with the help of a machine expert) [NM.6].

The components of the framework are briefly described as follows.

Defend: Initially, a thorough system analysis needs to be carried out to decide how best to build defensively against perceived threats and vulnerabilities; this includes a risk assessment in order to prioritize the assets in the system – which of them needs to be protected, and which of them most or least urgently, or using more or fewer resources. Building resilience into a system inevitably incurs costs, and these need to be carefully weighed. As a result of the system analysis, the system designer will propose a range of actions including building defensive walls (for example 'firewalls' to defend against cyber-attacks); adding some redundant links and nodes into the communications infrastructure; and at runtime, making appropriate adjustments such as firewall rules and resources.

Detect: The detect phase requires a monitoring system. Essentially, the network and/or networked system needs to be 'instrumented' so that the effects or symptoms of any challenge to the system's normal operation can be rapidly observed. This is sometimes called 'anomaly detection' or 'intrusion detection', and it has been the subject of much research in past decades [NM.2]. Nevertheless, it is difficult to distinguish the root cause of a challenge, and the detection may have to proceed without actually knowing for sure what is causing the problem. Typically, detected anomalies are classified and using this classification allows the next phase to be carried out.

Remediate: Remediation (or 'mitigation' as used by some resilience researchers) is the phase whereby some action is carried out to remove or improve the symptoms of a challenge or threat. In networked systems, it is typical to use 'traffic engineering' to improve the situation – for example, to remove or re-direct a particular stream of packets that come from a suspicious source in the network and that is adversely affecting a destination in the network such as a server that may be saturated with this traffic. Ideally, remediation should be done in real time, and it should be done autonomously, i.e. the resilience management mechanism makes the decision what to remediate and how and carries this out without human intervention. This is still a sensitive topic, and in existing systems the remediation will usually be carried out under the supervision of a human expert.

*Recover: I*n the recovery phase, the aim is to return the networked system to normal behavior if possible, and to try to make sure that the system takes account of the conditions that caused the anomalies. This implies some form of machine or human learning in order to improve the system's resilience. The recover activity should of course be carried out once the source of the challenge has been removed. Policies for high-level guidance may be used in this phase [NM.5].

Diagnose and Refine: The outer loop of the resilience strategy is an under-explored research area. The idea is that in future there will be a machine learning phase that steadily learns from previous experiences and builds up a body of expert knowledge on which to draw to improve the remediation and recovery activities and the resilience model that underlies them both. This requires providing real historical data for a DR prototype, and in turn the development of resilience subsystems that are subsequently deployed in the field. This raises a very important ethical question – for networked systems that operate critical infrastructures and services, should there always be a human in the loop.

17.4 Managing Diversified Resources

Driven by new technologies such as artificial intelligence, big data and the Internet of things, the future applications will be more diversified, and their requirements of computing resources are much differentiated. At the same time, more and more heterogeneous data is generated at the edge and the heterogeneous computing is arising to better serve personalized computing needs. In future networks, the unified management of heterogeneous computing resources and heterogeneous data is needed. The

main purpose is fulfilling diverse services requirements on computing and storage resources with the view of improving user experience, network efficiency and resource utilization.

In order to meet the needs of computation diversification, new hardware resources such as GPU, FPGA and other hardware for acceleration are introduced.

With the computation- intensive machine learning model training based on a large amount of data, AI proposes higher demand towards the data processing and computing power. As such the future edge deployment of AI needs heterogeneous computing hardware to support the resource-limited edge stations.

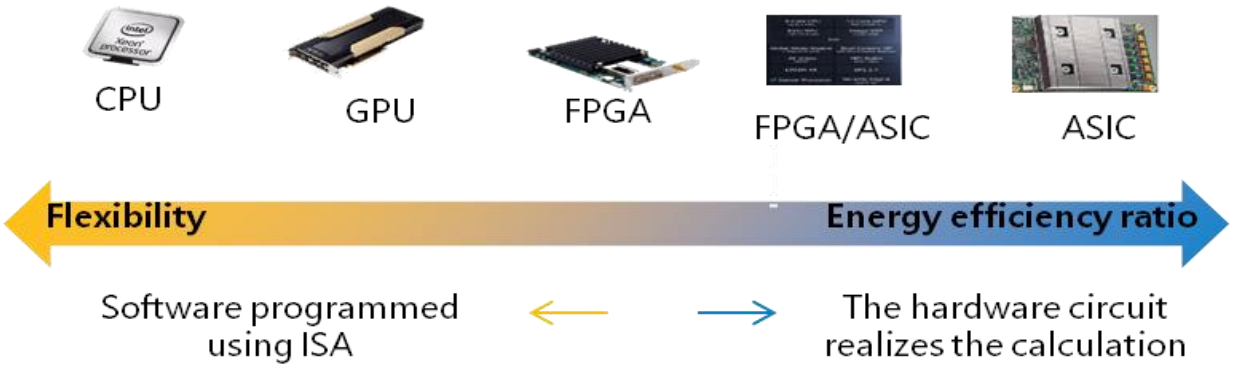


Figure 89–Heterogeneous computing hardware

It is necessary to research on the unified measurement of heterogeneous resources and build a unified resource view. What's more, the real-time update of the resource view is also required to achieve the timely and comprehensively aware of heterogeneous resources.

The centralized or distributed control and intelligent management over heterogeneous hardware could perform as the on-demand resource scheduling and data migration.

- Computing Resource measurement

  On the one hand, in the face of heterogeneous computing, the dimension of computing power's representation need to be studied to realize the perceptive and measurable computing power of the network and applications; on the other hand, how to measure the computing and storage power needed for specific application or service also needs to be studied.
- Computing Resource modelling

  The network node keeps information on currently deployed services and the performance and status of current computing resources and updates maintenance in real time.
- Computing Resource notification

  It is necessary to share and periodically update available computing power in network nodes so that other nodes in the network are aware of the specific configuration and real-time status of computing power.
- Coordination between Computing Resource and network resource

The research includes how to realize flexible traffic scheduling based on the coordination of network resources and computing resources, and to achieve the best user experience, computing resources utilization and network efficiency.

17.5 Knowledge Plane and Autonomic Management

The acquisition and use of expert knowledge in networks and networked systems has been hinted at in the Knowledge Plane proposal by David Clark and others [NM.3]; adopting and extending this idea should be investigated as an approach for building a situational awareness subsystem along with autonomic network and service management within the Network 2030 context. The resulting subsystem should be able to assist with the assurance of QoS and resilience by providing a measurement-based framework that informs management decisions.

Autonomic management is not only about having an autonomic network taking decisions by itself, but it is also about detecting failures, making improvements, and offering possibilities to the human being to take actions. It is also about predicting behaviors and changes that can enhance the system, for example using patterns [NM.7].

As shown in **Figure 90**, intents provided by the user (which could be the network Operator in Section 9) are passed to the Intent Plane, where the request is translated, normalized, decomposed and validated before it is transferred to the Management Plane. The Management Plane makes sure that there are enough resources available to answer the intent. It actively collects data from the Data Plane and uses techniques like continuous integration, continuous deployment (CI/CD) to ensure that the new intent will not adversely impact the existing intents in the system. Once the verification has been done, the new configuration will be delivered to the Control Plane to be applied.

In parallel to the user's intent, the system collects data from different sources (for example, weather, political or social networking information) and provides them to the Knowledge Plane as an input. The Knowledge Plane filters, adapts and classifies the data in the first place, then using for example big data algorithms, machine learning or deep learning, analyses and carries out some reasoning to predict actions and then applies them autonomously to the Management Plane, or else offers different possible behaviors to the Business Plane, where an appropriate or designated human can take the relevant actions.

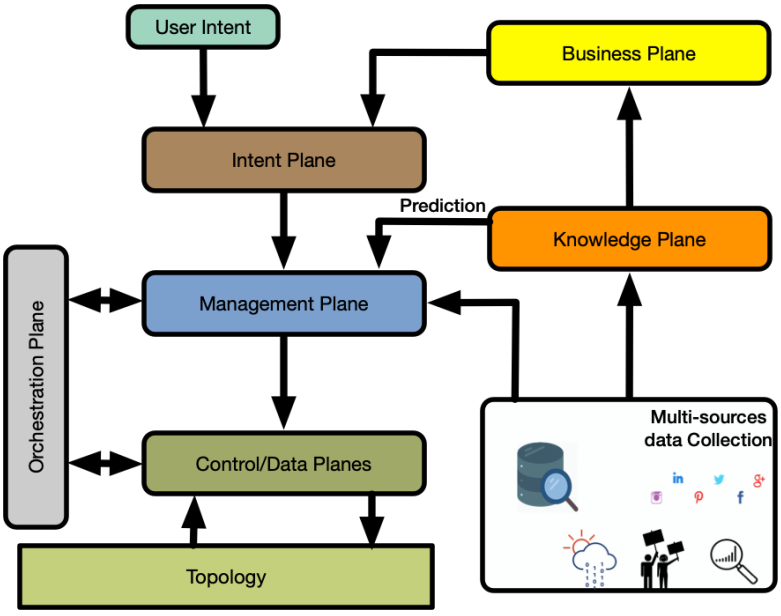


Figure 90–Automated, knowledge-based management

Our interpretation of the Knowledge Plane is depicted in **Figure 91**.

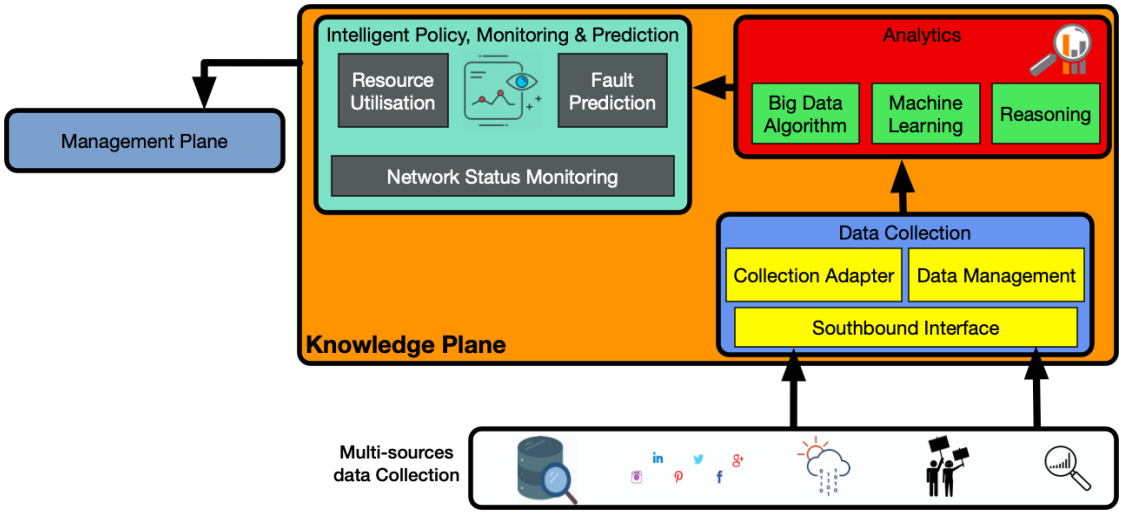


Figure 91–Knowledge Plane

17.6 Intent Management Framework

For future network 2030, improving the level of automation and intelligence has become the intrinsic demand for network management operation and maintenance. With key characterizes of intelligent and closed-loop intent assurance, Intent-Based Networking (IBN) can be a powerful solution to achieve in the context of Network 2030 predictive and protective autonomic management, including the specification of Quality of Service (QoS) and resilience covered in later sections.

Network2030 Management Architecture described in Section 4 is the automated and knowledge-based network management architecture consists of several planes including the intent plane. In this section,

we introduce an IBN framework for Network 2030 by describing the intent plane and different interactions with other planes. **Figure 92** introduces a high-level IBN framework, specifically, it shows the interaction between the intent plane and the other planes.

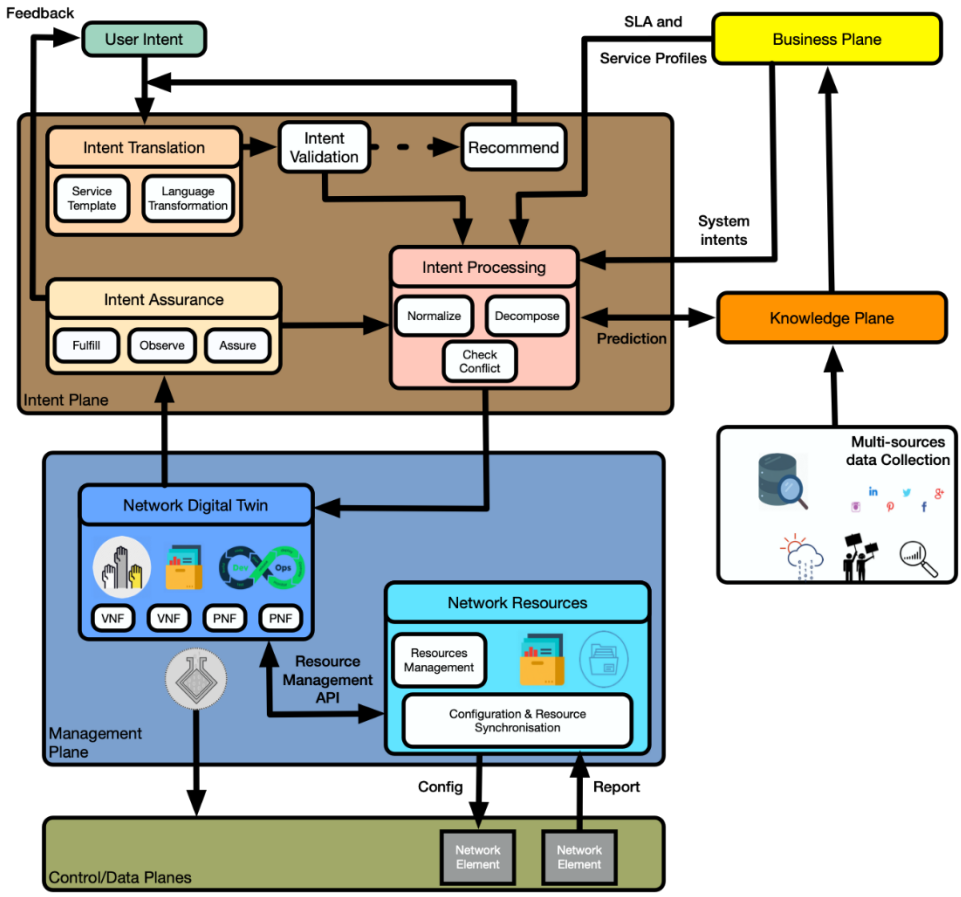


Figure 92–Framework of Intent-Based Networking for Network 2030

Intent-based management system is subject to a lifecycle as it changes over the course of time [NM.32]. This lifecycle is closely tied to various interconnection functions that are associated with the management concepts and operations. **Figure 93** depicts an Intent-based management system lifecycle and its main functions. These life-cycle functions are grouped into two (horizontal) functional artefacts, reflecting the distinction between fulfillment and assurance and into (vertical) three groups of artefacts: user-space, intend-base systems, network operation space.

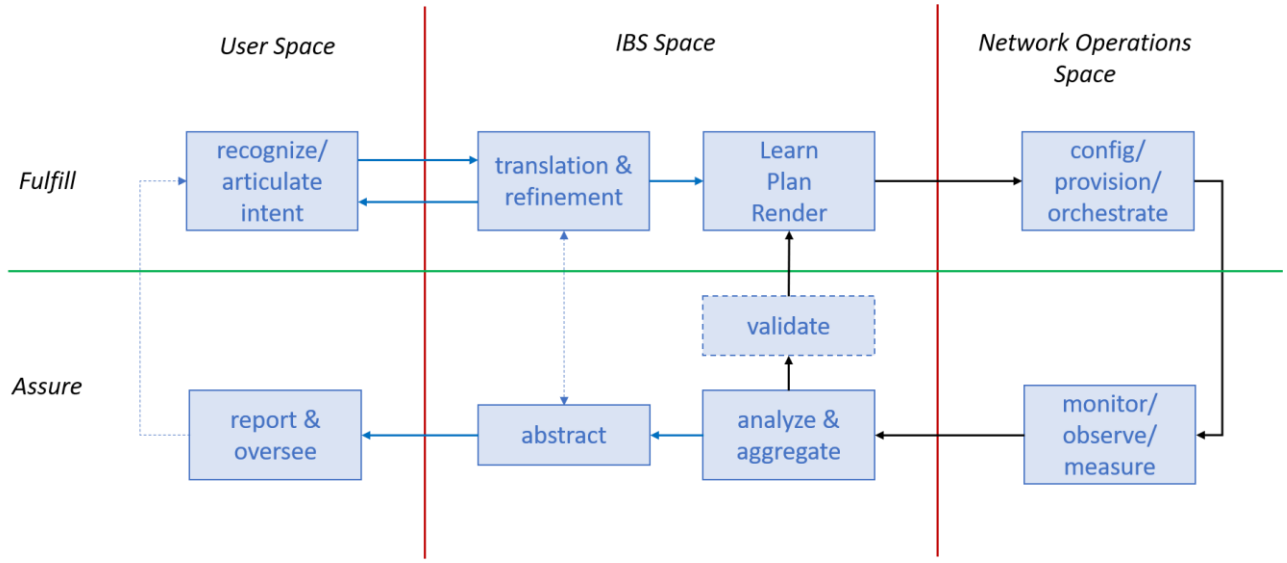


Figure 93–Intent-based Management Lifecycle

17.6.1 Intent Plane

The Intent Plane is decomposed to four main modules that translate, validate, decompose the original intent into network tasks, and keep track of its fulfilment once it is handed to the management plane.

- **Intent Translation**
  When an intent is exposed to the intent plane, the first module that deals with it is the "*Intent Translation*". Intention translation consists of mapping the intent from a certain high-level form to a more system-oriented request. This process can be done through a service template or a sort of language transformation.
- **Intent Validation**
  The "*Intent Validation*" module checks the syntax of the transformation and if everything is understandable to the system. If it is not the case, it can recommend a new syntax to the intent's originator. This micro-loop is the first control point to make sure that the intent can be processed correctly.
- **Intent Processing**
  Once the intent is validated, the "*Intent Processor*" takes into account the SLAs and service profiles (from the business plane) to normalize the intent and decompose it into small network tasks. It also checks if there are any conflicts with existing intents. The intent processing module interacts with the knowledge plane to analyze if any improvement can be done.
- **Intent Assurance**
  The "*Intent assurance*" module fulfills, observes, and assures in real-time whether the final result of the user's intent execution in network infrastructure meets the user's expectation. The intent assurance module interacts with the intent processing module and the network digital twin (from the management plane) in a closed-loop process of monitoring, tracking, diagnosing and restoring based on user intents.

17.6.2 Management Plane

The management plane is formed of two main modules that make sure that the new intent has enough available resources to run correctly and without affecting any existing and already running intents.

- **Network Resources**
  The "*Network Resources*" module collects lively data from the network elements and lists an up to date inventory of all available resources in the system. It communicates this information with the network digital twin through the resource management API, which helps the network digital twin to allocate properly the available resources for new requests.
- **Network Digital Twin**
  Using the available resources (from the network resources module) and DevOps techniques like continuous integration continuous deployment (CI/CD), the "*Network Digital Twin*" module creates a virtual real-time representation of the physical assets and builds and deploys virtually the new configurations (that answer the intent). Finally, it tests to be sure that the configuration is bugs-free, and the output corresponds to the requested intent. If the CI/CD technique validates the configuration, the code will be pushed for real deployment.

17.6.3 Intent Based APIs

In order to automate network management further, it is possible to offer user and administrative interfaces employing intent based APIs. A high-level intent based API architecture example is depicted in **Figure 94**.

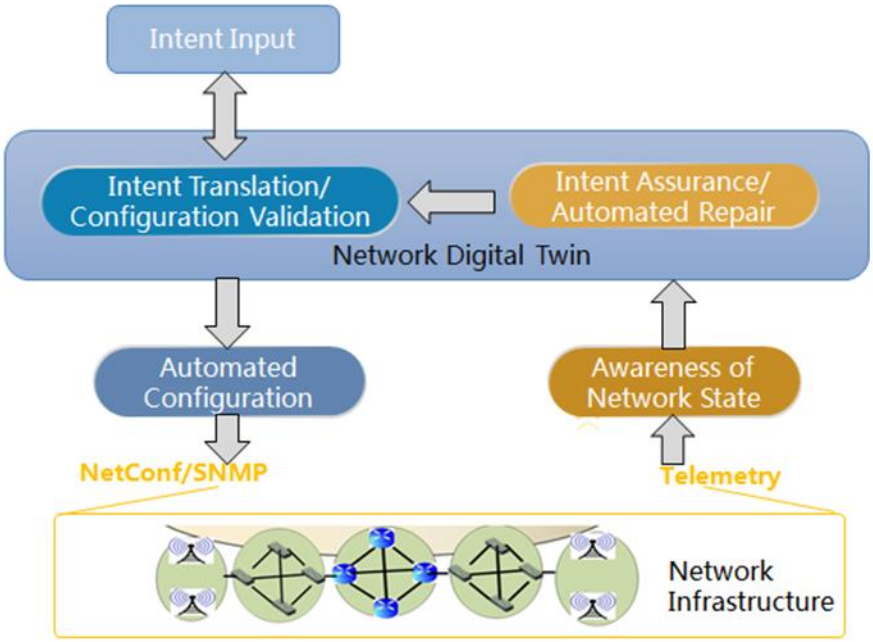


Figure 94–An Example Intent Based Networking implementation

The Intent input module is the end-user-oriented portal and the first step to realize the user's intention. The portal of intent input must be designed user friendly to get good user experience.

Intent input can use voice, icon drag and drop, design script import and other ways, user portal can be mobile APP, web pages, etc. Users should input their intents into IBN system in a concise and easy-to-use way, avoiding the use of a large number of professional CLIs and complex operations to ensure

user experience. Additionally, Intent input module can also capture intents dynamically from user's operations, using AI/ML technology. This can make user portal more concise and user-friendly.

When a user expresses a particular intention, different ways can be used, but IBN system should be able to transform from multiple intention input into a unique business policy, and pass this unique business strategy through standard interface to downstream intent translation and validation sub-module.

The implementation of the intent input module can also be predefined as a set of intents, including common business needs of users. Users need only select intent centrally when they intend to input, reducing the diversity of intent input and the difficulty of intent translation.

After intent translation and validation, there may be intent conflict. Therefore, the user intent input sub-module also needs to receive feedback from the intent translation sub-module, and make necessary amendments or adjustments to the intent.

Intention translation implements the conversion of business policies into network planning and device configuration. Then the configurations are validated on the simulation platform using digital twin technology. Common problems in device configuration can be detected in advance, e.g. address conflict, routing loop, inaccessibility of routing, and lack of resources.

Users concern the deployment of intents on the whole network. Business policies from intent input module are varied, which may be transient, persistent, simple, complex, device-level, network-level, etc. Intention translation module needs to decompose and translate all policies into device-oriented network planning and configuration. These configurations can form configuration files in the form of CLI, YANG model, script, etc. At the same time, the policy adjustment requirements from intent assurance and automated repair sub-module's feedback also need to be re-translated by intent translation sub-module to form an updated configuration file.

Intent translation generates a large number of configuration parameters, and the impact of this part of the configuration sent to the device is hard to be predicted. So, configuration validation can be simulated on the platform of network digital twin, which is virtual mirror of the network infrastructure.

Intent translation and configuration validation sub-module needs to ensure the integrity and implementability of user intents, and at the same time resolve intent conflicts caused by user negligence or other reasons. Some intent conflicts can be intelligently coordinated and resolved automatically by the system. In most cases, intent conflict needs to be fed back to the user, and the user clearly modifies the original intent to mitigate or resolve the conflict. As a supplement, the system can intelligently give one or several proposed intent modification schemes for users' reference, but ultimately it still needs users to make final decisions.

17.6.4 Business Plane

In our framework, the business plane represents the network's operator. It communicates existing SLAs and service profiles to the intent processing module in order to ensure that the new intents are not impacting the existing SLAs. From all information/predictions received from the knowledge plane, it also can generate and inject low-level intent to the system.

17.7 Compatibility with OSS/BSS

As described in **Figure 95**, each Operator providing a segment of Internet assigns an Orchestrator to manage all the resources and associated services in its domain and interoperate with Orchestrators of other Operators involved in the same service. Our management approach (intent-based, measurement-

based, emphasis on the business view, resilience and autonomic operation) is a progression from a classic OSS/BSS-based approach, and it can even be backward-compatible.

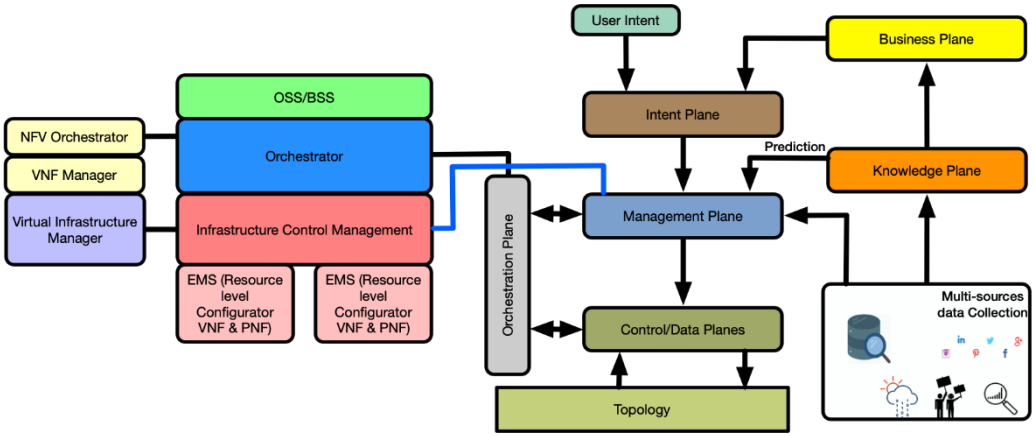


Figure 95–IBN interworking interfaces with OSS/BSS

17.8 AI/ML role in Management & Orchestration

Different artificial intelligence (AI) and machine learning (ML) techniques have been proposed and extensively developed for the materialization of the future networks in their different facets. The introduction of those ML techniques has become a necessity due to the complexity of future networks in order to supply the intended Future services [NM.11]. The scope of deployment Future networks ranges from an efficient use of the scarce radio resources to the proper management of the core network resources [NM.12]. The required flexibility, adaptability and programmability behavior can only be envisioned thanks to the use of artificial intelligence (AI) techniques [NM.13]. Those AI techniques will be responsible for the implementation of the management and orchestration modules, focusing on the execution of configuration and reconfiguration control loops, so necessary to simultaneously accommodate in an efficient way multiple tenants onto the same network infrastructure [NM.14].

Traditionally, machine learning techniques have been classified into supervised, unsupervised and reinforcement learning techniques [NM.11]. In its most extensive form, supervised and unsupervised techniques are used for the implementation of data classifiers, and with this purpose they have extensively been used in wired and wireless communication networks to implement traffic classification and prediction, fault-detection, intrusion-detection, anomaly-detection or channel and interference estimation. As a representative example, one of the main challenges of Future networks comes from the necessity to provide higher throughputs in more densified areas. In order to achieve that goal one possibility comes from the use of massive MIMO systems working with hundreds of antennas. That becomes a high-dimensional detection and channel estimation problem, which can be solved applying supervised learning [NM.15]. In spite of the usefulness of the supervised and unsupervised techniques, their scope is restricted to solving specific classification problems in the overall network infrastructure.

The reinforcement learning (RL) technique learns from experience by taking new actions to explore and increase its knowledge of the environment and uses a predefined goal to achieve its target in the long term, optimizing a given performance criterion. That is why RL has been used in those tasks devoted to tuning some working parameters targeted at the improvement of system performance, like the antenna tilt of the base stations [NM.16] or the transmitted power from the base stations [NM.17], or to decide with which base station (and using which communication technology) a new connection

will be set up [NM.18]. More recently, it has also been used to implement admission control mechanisms [NM.14] or resource orchestration [NM.19].

Also, the recent success in the development of deep learning techniques, as another form of supervised learning, has greatly contributed to the improvement of the RL technique. One of the main drawbacks of the RL technique came from the lack of stable training techniques when using approximation functions as a substitute of the traditional Q-table used with the Q-Learning technique. Nevertheless, when trying to notably increase the number of states or actions, the use of tables becomes impractical, and there was no way to achieve a stable training behavior when using neural networks as approximation functions. Presently, thanks to the use of deep learning techniques, that drawback has been overcome, achieving not only the practical implementation of deep Q networks, but also directly learning action policies without using the Q-Learning technique, for both, discrete and continuous actions [NM.20].

Machine intelligence encompasses advanced machine learning algorithms that can rapidly correlate information from multiple data sets in order to extract real-time insights for driving network and service orchestration. Cognitive AI techniques that emulate the decision-making processes of the human mind will be applied for automating operator workflows. Due to the promising possibilities of Deep Reinforcement Learning techniques, we envisage a successful approach using these techniques for the implementation of the intelligence within the Network 2030 architecture. The diversity of specific requirements due to the increasing complexity of the services to be demanded by the future service tenants' results in an even more complex implementation of the management and orchestration functionality. In order to cope with that complexity, and to also provide a scalable solution, presently only a deep reinforcement learning approach is foreseen as a plausible alternative. The use of deep learning in networking is not straightforward. Although it has been used successfully in other AI & ML techniques would need to be adapted to the specific context of problems addressed in Network2030. As such, it will constitute one of the major research challenges in Network 2030.

.

17.8.1 Network Logical Architectural Integration of multiple AI/ML methods

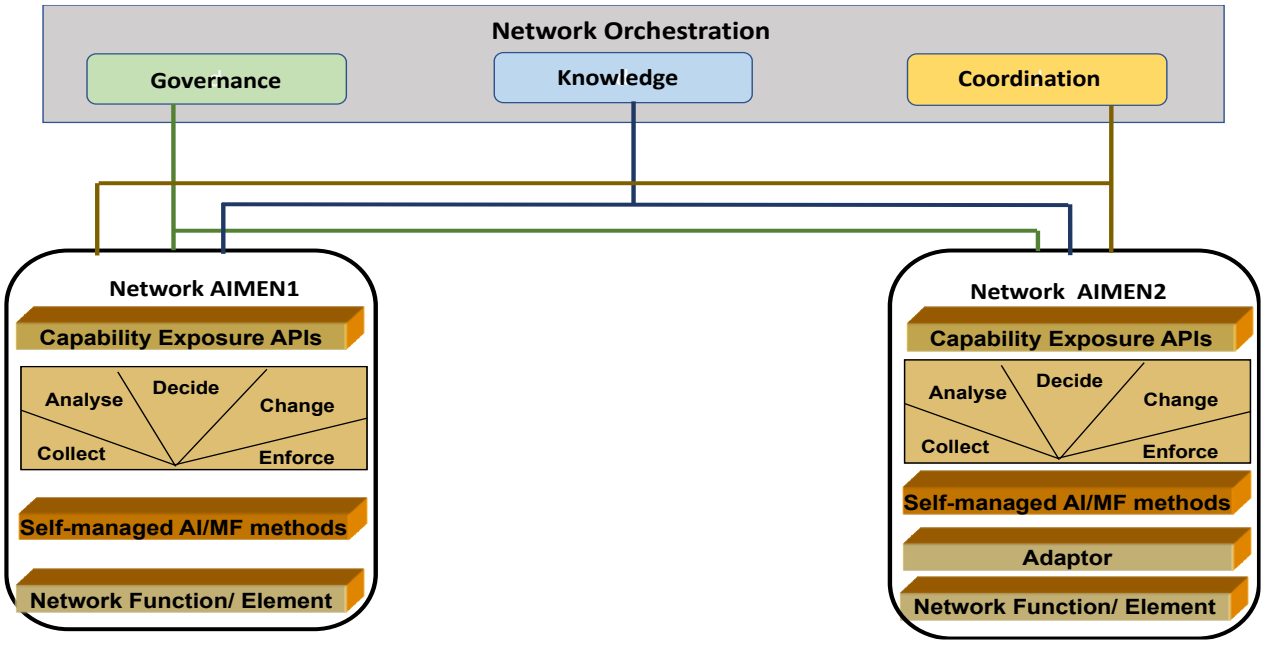


Figure 96 - Logical Architecture – Network Integration with multiple AI/ML Methods

A set of concepts related to AI/MF life cycle and its interaction with its network context is depicted in **Figure 96** as follows:

- A **Network AI/MF Empowerment Method (AIMEM)** is a piece of software that contains the logic achieving a specific autonomic function specified by AI/MF specific methods. Such software is deployed in a network system and requires being instantiated on a set of concrete network elements or Network functions to effectively perform its functionality.

- An **instance of a given AIMEN class** performs a given function onto a given sub-set of network elements. This is achieved by binding the code of an AIMEN class to a set of identified network resources/network functions. This AIMEN instance is identified by an instance ID and its unique interface with the Network Orchestration. This AIMEN instance at any given time is handling a set of identified network resources (this set can evolve with time). Hence, there may be multiple instances of a given AIMEN class inside the same network (e.g. one per domain). An AIMEN instance is managed by the Management & Orchestration system as an atomic entity, while its internal functioning can rely on separated pieces of software running on different Network Functions (NF).

The **machine-readable descriptions of the above concepts** are explained below:

A given AIMEN manifest provides guidance to the network operator in order to install and configure an instance of this AIMEN class.

- **The AIMEN instance sends this description** towards Management and Orchestration system. This description is used for registration of the NET_AI/MF_EM. It tells which information is monitored and which range of actions can be taken. It provides AIMEN instance information when starting, in order to register: (1) Capabilities of this AIMEN instance regarding information/knowledge sharing; (2) Requirements of this AIMEN instance regarding knowledge inputs; (3) Conflicts of this AIMEN instance with already running AIMEN instances of any AIMEN class.

- **An AIMEN mandate** is a set of instructions telling which network functions or services must be handled by this AIMEN instance and which settings this AIMEN instance MUST work with.

To illustrate the previous definitions, let us sketch a very simplified **AIMEN Life cycle** process used to start an AI/MF method (coming as an AIMEN class) inside a Network system.

- First, the software corresponding to the AIMEN class is being installed on the relevant machines/network functions (helped in this by the indications available in the AIMEN Manifest).

- Second, the Network Orchestration is demanding to the installed software the creation of an AIMEN instance. Then the Orchestration block sends a mandate for the AIMEN instance to deploy itself. The process ends with an AIMEN instance ready to register to Management and Orchestration.

- Third, this AIMEN instance is sending its AIMEN instance description to the all Orchestration functions (Governance, Coordination, Knowledge) in order to [NM.20] complete registration. Once the registration is successfully completed, the AIMEN instance is ready to start upon command from the Orchestration. This process is part of what it is called the AIMEN lifecycle which is illustrated in **Figure 97**.

This process is repeated when AIMEN functionality is concatenated as a pipeline across different domains (i.e. operator administrative domains, Access/Core/Edge domains) [NM.29]. The following concepts are identified:

Chaining is the process of connecting AI/ML functions together to form a complete e-2-e AI/ML pipeline.

Intent - a declarative mechanism which is used by network operator to specify the machine learning use case.

Source - this node is the source of data that can be used as input for the AI/ML function.

Collector/Aggregator/Distributor - this node is responsible for collecting data from the Source. It is responsible for aggregating data and for distributing the AI/ML output to the corresponding sinks

Sink - this node is the target of the AI/ML output, on which it takes action (e.g. adjusting the measured KPIs periodicity based on AI/ML output)

The flow of information in an AI/ML-based use case can be represented by an AI/ML pipeline – **Figure 97**. The data collected at various collection points (**Source**) need to be gathered (by a **Collector**), processed (by an **Aggregator**) and distributed (by a **Distributor**) before feeding these data to the AI/ML method. The output of the AI/ML method is then activated / implemented in sink points (**Sink**).

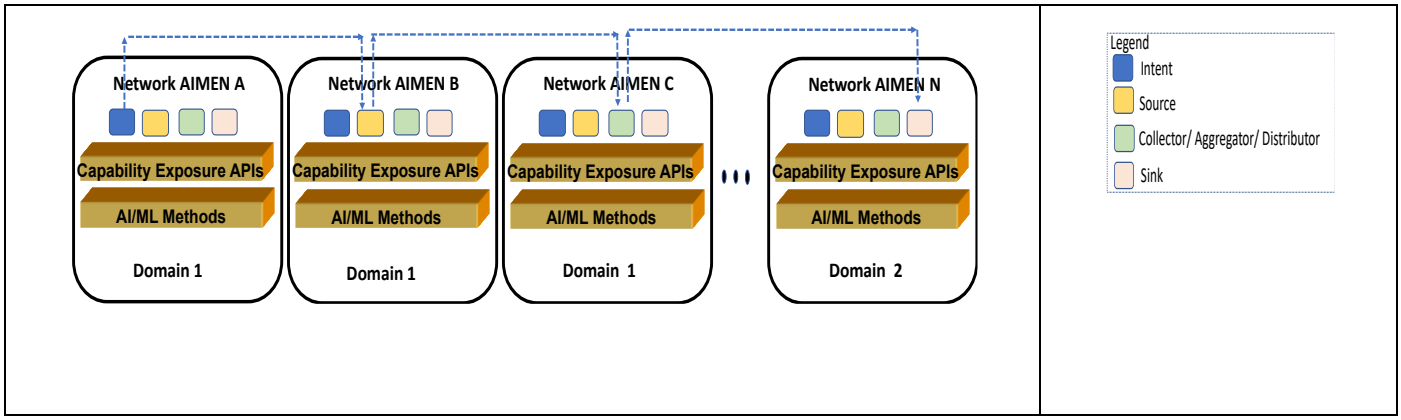


Figure 97- - Chaining AI/ML functions together: Multi -domain AI/ML Pipeline

17.9 Conclusion

This section has presented new contributions to network management that are appropriate for Network 2030, focusing on an intent-based approach that features autonomic management and makes extensive use of measurements. The approach emphasizes the need to support QoS via resilience management, the management of diversified resources, and the use of a knowledge plane for autonomic operation. Compatibility with OSS/BSS is explained, and finally the role of AI/ML in management and orchestration is introduced and outlined.

18 Quantum Computing and Its Impact

Quantum Computing is the use of quantum-mechanical phenomena such as superposition and entanglement to perform computation. Computers that perform quantum computation are known as quantum computers [QUANTUM.1]. Quantum computers are believed to be able to solve certain computational problems, such as integer factorization, substantially faster than classical computers.

According to [QUANTUM.2, QUANTUM.3], the Google quantum computer performed in 3 minutes 20 seconds a mathematical calculation that supercomputers could not complete in under 10,000 years.

In classical computers, the information is represented in bits (i.e. 1s and 0s). For example, hard drives store documents by locking magnets in either the up or down position. In Quantum computers, the information is represented in quantum bits or qubit. Qubits represent the information based on the behavior of atoms, electrons, and other particles, objects governed by the rules of quantum mechanics. A hard drive magnet must always point up or down, for instance, but an electron's direction is unknowable until measured: the electron behaves in such a way that describing its orientation requires a more complex concept — known as superposition — that goes beyond the straightforward labels of "up" or "down."

Quantum particles can also be yoked together in a relationship called entanglement, such as when two photons (light particles) shine from the same source. Pairs of entangled particles share an intimate bond akin to the relationship between the two faces of a coin — when one face shows heads the other displays tails. Unlike a coin, however, entangled particles can travel far from each other and maintain their connection.

Entangled photons were sent over fiber-optic cables connecting Brookhaven National Laboratory in New York with Stony Brook University, a distance of about 11 miles [QUANTUM.4]. The wireless transmission of entangled photons over a similar distance through the air is also tested.

It remains to be seen whether commercial computers and transmission devices based on quantum computing will be available in 2030 or not. However it is clear that quantum computing will revolutionize networking along with Artificial Intelligence and Machine Learning techniques.

For example, we expect networks to be much more decentralized. Cross-switch delays of network elements may be reduced from miliseconds to nanoseconds. With large computing power, we will be able to represent objects much more precisely. The communications will become richer.

With Quantum Computing, we expect Network2030 to become fully automated and self-managed by being able to store and process large amount of connectivity, application and management information of a domain in a computer, instead of a number of networked computers in one or more data centers.

19 Conclusion

This technical specification describes a vision of an architecture and its details for public networks in the year 2030 and beyond, namely Network2030. Network2030 is an automated federation of heterogeneous networks that can support services requiring stringent SLOs and bandwidth in Gbps and Tbps, in addition to supporting best effort services.

Although it is always difficult to predict the future, automation, self-management, decentralization, data transmission in much larger bandwidth are expected to be the key characteristics of Network2030. It is hoped that this specification provides guidance in planning Network2030.

Bibliography

[GEN.1] "IoT to drive growth in connected devices through 2022: Cisco", www.zdnet.com, Nov 27, 2018

[GEN.2] "100 Billion IoT Connected Devices will be Installed by 2025", www.sdcexec.com, March 10, 2017.

[GEN.3] A. Patrizio, " IDC: Expect 175 zettabytes of data worldwide by 2025", Network World, December 3, 2018

[Sub-Group 1.1] "Second Sub-G1 report as an update of "Use cases and network requirements for Network 2030", June 2020.

[Sub-Group 2.1] "Description of New Services and Capabilities for Network 2030: Technical Gap and Performance Target Analysis", June 2020.

[Sub-Group 2.2] "Gap Analysis of New Services, Capabilities and Use cases for the Networks in 2030 or Beyond (or Network 2030) ", June 2020.

[ITU-T.1] IMT-O-042 "Draft Recommendation: Requirements of IMT-2020 from network perspective", December 2016.

[ITU-T.2] IMT-O-043 "Draft Recommendation: Framework of IMT-2020 network architecture", December 2016.

[PRINCIPLE.1] R. Bushe, D. Meyer, RFC3439- Some Internet Architectural Guidelines and Philosophy -https://tools.ietf.org/html/rfc3439

[PRINCIPLE.2] Pit and Quarry Magazine, Vol. 63, July 1970, p.172, quote: "as in every other step of the development process, follow the KISS principle — Keep It Simple, Stupid."

[ARCH.1] M. Toy, "Cloud Services Architectures", Procedia Computer Science 61 (2015) 213 – 220

[ARCH.2] M. Toy, "Cloud Services Architecture", MEF68 Draft Specification, May 2020.

[ARCH.3] ETS GR NFV-EVE016 "Connection-based Virtual Services", May 2020.

[ARCH.4] MEF 55 "Lifecycle Service Orchestration (LSO): Reference Architecture and Framework", March 2016.

[ARCH.5] MEF 55.1 Draft "Revised Lifecycle Service Orchestration (LSO): Reference Architecture and Framework", May 2020.

[ARCH.6] M. Toy, "Self-managed Networks with Fault Management Hierarchy", Procedia Computer Science, Volume 36, 2014, Pages 373-380

[ARCH.7] M. Toy, "OCC 1.0 Reference Architecture", December 2014. https://wiki.mef.net/display/OCC/OCC+Specifications?preview=%2F63185562%2F63342484%2FOCC+1.0+Reference+Architecture.pdf

[EDGE.1] https://forge.etsi.org/

[EDGE.2] GSMA Operator Platform Concept, https://www.gsma.com/futurenetworks/resources/operator-platform-concept-whitepaper

[EDGE.3] ETSI MEC in 5G networks https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

[NS-1]. Programmable Networks for IP Service Deployment" Galis, A., Denazis, S., Brou, C., Klein, C.–"ISBN 1-58053-745-6, pp 450, June 2004, Artech House Books, http://www.artechhouse.com/International/Books/Programmable-Networks-for-IP-Service-Deployment-1017.aspx

[NS-2]. "Management and Service-aware Networking Architectures (MANA) for Future Internet" – A. Galis et all - Invited paper IEEE 2009 Fourth International Conference on Communications and Networking in China (ChinaCom09) 26-28 August 2009, Xi'an, China, http://www.chinacom.org/2009/index.html

[NS-3]. "The RESERVOIR Model and Architecture for Open Federated Cloud Computing", Rochwerger, J. Caceres, R. Montero, D. Breitgand, A. Galis, E. Levy, I. Llorente, K. Nagin, Y. Wolfsthal - IBM System Journal Special Edition on Internet Scale Data Centers, vol. 53, no. 4, 2009, http://www.haifa.ibm.com/dept/stt/sas_public.html,

[NS-4]. "Infrastructure Slicing Landscape: –Galis. A, Makhijani, K - Tutorial at IEEE NetSoft 2018, Montreal 19 July 2018; http://discovery.ucl.ac.uk/10051374/

[NS-5]. "Perspectives on Network Slicing – Towards the New 'Bread and Butter' of Networking and Servicing"– Galis. A January 2018 https://sdn.ieee.org/newsletter/january-2018/perspectives-on-network-slicing-towards-the-new-bread-and-butter-of-networking-and-servicing

[NS-6] ITU-T Y.3011- http://www.itu.int/rec/T-REC-Y.3001-201105-I

[NS-7]. IETF draft "Network Slicing" Galis., A, Dong., J, Makhijani, K, Bryant, S., Boucadair, M, Martinez-Julia, P. https://tools.ietf.org/html/draft-gdmb-netslices-intro-and-ps-01

[NS-8] IETF draft (2017) "Network Slicing" Galis., A, Dong., J, Makhijani, K, Bryant, S., Boucadair,

[NS-9] 3GPP 2019 Specification 28 554

[NS-10] Kuklinski, S. and Tomaszewski, L. (2019). Key performance indicators for 5G network slicing. 2nd Workshop on Advances in Slicing for Softwarized Infrastructures, Paris, France, 28th June 2019.

[NS-11] http://groups.geni.net/geni/wiki/GENIConcepts

[NS-12] ITU-T Y.3011- http://www.itu.int/rec/T-REC-Y.3001-201105-I

[NS-13] ITU-T IMT 2020 Technical Report: Application of network softwarization to IMT-2020 (O-041) - https://www.itu.int/en/ITU-T/focusgroups/imt-2020/Pages/default.aspx

[NS-14] ITU-T Recommendation on Network Slicing ITU-T Y.3112

[NS-15] 3GPP TR23.799 https://www.3gpp.org/DynaReport/23-series.htm

[NS-16] 3GPPPTR28.801 https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3091

[NS-17] 3GPPPTR28.8043 https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3549

[NS-18] 3GPPP TR28.811 https://portal.3gpp.org/desktopmodules/Specifications/pecificationDetails.aspx?specificationId=3717

[NS-19] 3GPPPTS28.201 https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3692

[NS-20] 3GPPPTS28.202 https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3684

[NS-21] GSMA Network Slicing https://www.gsma.com/futurenetworks/ip_services/understanding-5g/network-slicing/

[NS-22] NGMN –White Paper description of network for service provider networks https://www.ngmn.org/fileadmin/user_upload/161010_NGMN_Network_Slicing_framework_v1.0.8.pd

[NS-23] ETSI E2E network slicing reference framework and information model. Kiran, Makhijani, Kevin Smith, John Grant, Alex Galis-UCL, Xavier Defoy-Interdigital published in October 2018 by ETSI as a standard specification document. https://www.etsi.org/deliver/etsi_gr/NGP/001_099/011/01.01

[NS-24] ETSI Multi-access Edge (MEC) support for slicing https://www.etsi.org/deliver/etsi_gr/MEC/001_099/024/02.01.01_60/gr_MEC024v020101p.pdf

[NS-25] ETSI Zero Touch Network (ZTN) https://www.etsi.org/technologies/zero-touch-network-service-management

[NS-26] ONF TR-526: "Applying SDN architecture to 5G slicing", Issue 1, https://www.opennetworking.org;
[NS-27] SDN Architecture - https://www.opennetworking.org/wp-content/uploads/2014/10/TR-521_SDN_Architecture_issue_1.1.pdf
[NS-28] BBF https://www.broadband-forum.org/5g SD-406: End-to-End Network Slicing
[NS-29] MEF SD-WAN https://www.mef.net/resources/technical-specifications/download?id=122&fileid=file1
[NS-30] ITU-T Network 2030 “New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis” https://www.itu.int/en/ITU-T/focusgroups/Network2030/Documents/Deliverable_NETWORK2030.pdf
[NS-31] GSMA NG.116 Generic Network Slice Template v2.0 - https://www.gsma.com/newsroom/all-documents/generic-network-slice-template-v2-0/
[NM.1] [Campbell] Campbell, A., Coulson, G., Hutchison, D. A Quality of Service Architecture. ACM SIGCOMM Computer Communication Review 24 (2), 1994, pp. 6-27.
[NM.2] [Chandola] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM computing surveys (CSUR)*, *41*(3), 15.
[NM.3] [Clark] Clark, D.D., Partridge, C., Ramming, J.C., & Wroclawski, J. (2003). A knowledge plane for the internet SIGCOMM 2003, DOI:10.1145/863955.863957
[NM.4] [Dobson] Dobson, S., Hutchison, D., Mauthe, A. U., Schaeffer-Filho, A. E., Smith, P. & Sterbenz, J. PG. (2019), Self-Organization and Resilience for Networked Systems: Design Principles and Open Research Issues 1/04/2019, In : Proceedings of the IEEE. 107, 4, p. 819-834 16 p.
[NM.5] [Gouglidis] Gouglidis, A., Hu, V. C., Busby, J. S., & Hutchison, D. (2017). Verification of resilience policies that assist attribute-based access control. In Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control (pp. 43-52). ACM.
[NM.6] [Hutchison] Hutchison, D., & Sterbenz, J. P. (2018). Architecture and design for resilient networked systems. Computer Communications, 131, 13-21.
[NM.7] [Smith] Smith, P., Schaeffer-Filho, A., Hutchison, D. & Mauthe, A., Management patterns: SDN-enabled network resilience management. Network Operations and Management Symposium (NOMS), 2014 IEEE. IEEE, pp.1-9.
[NM.8] [Sterbenz] Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, *54*(8), 1245-1265.
[NM.9] [Yeadon] Yeadon, N, Mauthe, A., Garcia, F. Hutchison, D. QoS filters: Addressing the heterogeneity gap Interactive Distributed Multimedia Systems and Services (IDMS), 1996, pp. 227-243.
[NM.10] [Intent functions] https://tools.ietf.org/html/draft-irtf-nmrg-ibn-concepts-definitions-00
[NM.11] [Jiang] Jiang, Chunxiao, et al. "Machine learning paradigms for next-generation wireless networks." IEEE Wireless Communications 24.2 (2017): 98-105.
[NM.12] [Li] Li, Rongpeng, et al. "Intelligent 5G: When cellular networks meet artificial intelligence." IEEE Wireless Communications 24.5 (2017): 175-183.
[NM.13] [Gutierrez-Estevez] Gutierrez-Estevez, David M., et al. "The path towards resource elasticity for 5g network architecture." 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). IEEE, 2018

[NM.14] [Raza] Raza, Muhammad Rehan, et al. "A slice admission policy based on reinforcement learning for a 5g flexible ran." 2018 European Conference on Optical Communication (ECOC). IEEE, 2018.

[NM.15] [Wen] C.-K. Wen et al., "Channel Estimation for Massive MIMO Using Gaussian-Mixture Bayesian Learning," IEEE Trans. Wireless Commun., vol. 14, no. 3, Mar. 2015, pp. 1356–68.

[NM.16] [Razavi] Razavi, Rouzbeh, Siegfried Klein, and Holger Claussen. "Self-optimization of capacity and coverage in LTE networks using a fuzzy reinforcement learning approach." 21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. IEEE, 2010.

[NM.17] [Dirani] Dirani, Mariana, and Zwi Altman. "A cooperative reinforcement learning approach for inter-cell interference coordination in OFDMA cellular networks." 8th International Symposium on Modelling and Optimization in Mobile, Ad Hoc, and Wireless Networks. IEEE, 2010.

[NM.18] [Kudo] Kudo, Toshihito, and Tomoaki Ohtsuki. "Cell range expansion using distributed Q-learning in heterogeneous networks." EURASIP Journal on Wireless Communications and Networking2013.1 (2013): 61.

[NM.19] [Chen] Chen, Xianfu, et al. "Multi-tenant cross-slice resource orchestration: A deep reinforcement learning approach." arXiv preprint arXiv:1807.09350 (2018).

[NM.20] [Mnih] Mnih, Volodymyr, et al. "Asynchronous methods for deep reinforcement learning." International conference on machine learning. 2016.

[NM.21] [ITU-T IMT2020 results] (https://www.itu.int/en/ITU-T/focusgroups/imt-2020/Pages/default.aspx):

[NM.22] O-041-Network Softwarization.docx

[NM.23] O-043-Network Architecture.docx

[NM.24] O-046-Network Management Requirements.docx

[NM.25] O-047-Network Management Framework.docx

[NM.26] [ITU-T IMT2020 Recommendations]

[NM.27] Y.3111 - IMT-2020 network management and orchestration framework

[NM.28] Y3100 – IMT2020 network: Terms and definitions

[NM.29] [ITU-T FG-ML5G-ARC5G] Unified architecture for machine learning in 5G and future networks.

[NM.30] [IOAM] Brockners F, S. Bhandari, C. Pignataro, H. Gredler, J. Leddy, S. Youell,T. Mizrahi, D. Mozes, P. Lapukhov, R. Chang, D. Bernier, J. Lemon: "Data Fields for In-situ OAM," IETF Internet Draft draft-ietf-ippm-ioam-data, July 2019.

[NM.31] [Fioccola] Fioccola G, A. Capello, M. Cociglio, L. Castaldelli, M. Chen, L. Zheng, G. Mirsky, T. Mizrahi: "Alternate-Marking Method for Passive and Hybrid Performance Monitoring," RFC 8321, IETF, January 2018.

[NM.32] A. Clemm, et. al. "Intent-Based Networking - Concepts and Definitions", https://tools.ietf.org/html/draft-irtf-nmrg-ibn-concepts-definitions-01

[ROUT.1] M. Handley, *Delay is Not an Option: Low Latency Routing in Space*, ACM HotNets 2018

[ROUT.2] G. Giuliari, T. Klenze, M. Legner, D. Basin, A. Perrig, & A. Singla, *Internet backbones in space,* ACM SIGCOMM Computer Communication Review, Vol. 50, No. 1, 2020.

[ROUT.3] Z. Yang, Q. Wu, H. Li, J. Wu, *A Space-Terrestrial network integration routing protocol: NTD-BGP*, Journal Tsinghua Univ (Sci & Technol), Vol. 59, No. 7, 2019.

[ROUT.4] S. Liu, X, Hu, Y. Wang, G. Cui, W. Wang, *Distributed Caching Based on Matching Game in LEO Satellite Constellation Networks*, IEEE Communication Letters, Vol. 22, Issue 2, 2017

[ROUT.5] A. Kaloxylos, *A Survey and an Analysis of Network Slicing in 5G Networks*, IEEE Communications Standards Magazine, Vol. 2, Issue 1, 2018

[ROUT.6] [PPR] IEEE Global Communications Conference (GLOBECOM): "Preferred Path Routing - A Next-Generation Routing Framework Beyond Segment Routing", U. | Chunduri, A. Clemm, R. Li, 2018, Abu Dhabi, UAE, December 2018.

[ROUT.7] [PLFA] Preferred Path Loop-Free Alternate (pLFA) - https://tools.ietf.org/html/draft-bryant-rtgwg-plfa-00

[ROUT.8] [PPR-Graph] https://datatracker.ietf.org/doc/draft-ce-lsr-ppr-graph/

[ROUT.9] https://datatracker.ietf.org/meeting/103/materials/slides-103-rtgarea-rift-update Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001, <https://www.rfc-editor.org/info/rfc3209>.

[ROUT.10] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[ROUT.11] https://datatracker.ietf.org/doc/draft-ietf-rtgwg-segment-routing-ti-lfa/

[ROUT.12] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/xe-3s/iri-xe-3s-book/iri-ip-lfa-frr.html

[ROUT.13] Shand, M. and S. Bryant, "IP Fast Reroute Framework", RFC 5714, DOI 10.17487/RFC5714, January 2010, <https://www.rfc-editor.org/info/rfc5714>.

[ROUT.14] Shand, M. and S. Bryant, "A Framework for Loop-Free Convergence", RFC 5715, DOI 10.17487/RFC5715, January 2010, <https://www.rfc-editor.org/info/rfc5715>.

[ROUT.15] SCION: https://www.scion-architecture.net

[ROUT.16] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

[ROUT.17] [ICSO] Assessment of the effective performance of DPSK vs. OOK in satellite-based optical communications, ICSO 2018, https://doi.org/10.1117/12.2536128

[ROUT.18] [Miller] Miller, Peter. "Ka-Band – the future of satellite communication" http://www.tele-satellite.com/TELE-satellite-0709/eng/feature.pdf

[ROUT.19] Giacomo Giuliari, Tobias Klenze, Markus Legner, David Basin, Adrian Perrig and Ankit Singla. Internet Backbones in Space. In ACM SIGCOMM Computer Communications Review, 50(1), 2020.

[ROUT.20] TS 23.501 System architecture for the 5G System (5GS)

[ROUT.21] Robert Lychev, Sharon Goldberg, and Michael Schapira. Is the Juice Worth the Squeeze? BGP Security in Partial Deployment. In Proceedings of ACM SIGCOMM, August 2013.

[ROUT.22] Matthias Hollick, Cristina Nita-Rotaru and Panagiotis Papadimitratos, Adrian Perrig, and Stefan Schmid. Toward a Taxonomy and Attacker Model for Secure Routing Protocols. In ACM SIGCOMM Computer Communication Review, 47(1), 2017.

[ROUT.23] Amir Herzberg1, Matthias Hollick, and Adrian Perrig. Report from Dagstuhl Seminar 15102, Secure Routing for Future Communication Networks. Dagstuhl Reports, 5(3):28-40, 2015, ISSN 2192-5283. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik. DOI: 10.4230/DagRep.5.3.28.

[ROUT.24] Danny Cooper, Ethan Heilman, Kyle Brogle, Leonid Reyzin, and Sharon Goldberg. On the Risk of Misbehaving RPKI Authorities. In Proceedings of ACM HotNets-XII, November 2013.

[ROUT.25] Adrian Perrig, Pawel Szalachowski, Raphael M. Reischuk, and Laurent Chuat. SCION: A Secure Internet Architecture. Springer International Publishing AG, 2017.
[ROUT.26] https://www.manrs.org/
[ROUT.27] Yuan, X., "On Nonblocking Folded-Clos Networks in Computer Communication Environments", IEEE International Parallel & Distributed Processing Symposium, 2011.
[ROUT.28] Apache Software Foundation, "Thrift Interface Description Language", <https://thrift.apache.org/docs/idl>.
[ROUT.29] https://datatracker.ietf.org/wg/rift/about/
[ROUT.30] https://datatracker.ietf.org/wg/lsvr/about/
[ROUT.31] https://datatracker.ietf.org/meeting/103/materials/slides-103-rtgarea-lsvr-update
[ROUT.32] https://www.scion-architecture.net/pdf/2017-SCION-CACM.pdf

[SEC.1] Adrian Perrig, Pawel Szalachowski, Raphael M. Reischuk, and Laurent Chuat. SCION: A Secure Internet Architecture. Springer International Publishing, 2017.
[SEC.2] SCION Control-Plane PKI. Accessed in March 2020 at: https://github.com/scionproto/scion/blob/master/doc/ControlPlanePKI.md
[SEC.3] Liu Bingyang, Yang Fei, Ren Shoushou, Wei Xinpeng, Yang Xue, Wang Chuang, and Yan Zhiwei. Decentralized Internet Infrastructure (去中心化互联网基础设施). Telecommunication Science (电信科学). 2019. Online: http://www.infocomm-journal.com/dxkx/article/2019/1000-0801/1000-0801-35-8-00074.shtml
[SEC.4] Jiang Weiyu, Liu Bingyang, and Wang Chuang. Network Architecture with Inherent Security Features (内生安全网络架构). Telecommunication Science (电信科学). 2019. Online: http://www.infocomm-journal.com/dxkx/article/2019/1000-0801/1000-0801-35-9-00020.shtml
[SEC.5] Taeho Lee, Christos Pappas, David Barrera, Pawel Szalachowski, and Adrian Perrig. Source accountability with domain-brokered privacy. Proceedings of the 12th International on Conference on emerging Networking EXperiments and Technologies. 2016.
[SEC.6] Benjamin Rothenberger, Dominik Roos, Markus Legner, and Adrian Perrig. PISKES: Pragmatic Internet-Scale Key Establishment System. Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS). 2020.
[QoS.1] TS 23.401 General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
[QoS.2] TS 23.501 System architecture for the 5G System (5GS)
[QoS.3] “Common Public Radio Interface: eCPRI Interface Specification”, http://www.cpri.info/downloads/eCPRI_v_1_0_2017_08_22.pdf
[QoS.4] Transport Aware Mobility for 5G - https://tools.ietf.org/html/draft-clt-dmm-tn-aware-mobility-04
[QoS.5] Ingo Busse, Bernd Deffner, Henning Schulzrinne, “Dynamic QoS control of multimedia applications based on RTP”, Computer Communications, Volume 19, Issue 1, 1996, Pages 49-58, ISSN 0140-3664
[QoS.6] X. Zhu, R. Pan, M. Ramalho, S. Mena, "Network-Assisted Dynamic Adaptation (NADA): A Unified Congestion Control Scheme for Real-Time Media", RFC8698, Feb. 2020
[QoS.7] Andrew Campbell, Geoff Coulson, David Hutchison. "A quality of service architecture". SIGCOMM Comput. Commun. Rev.24, 2 (April 1994), 6–27. DOI: https://doi.org/10.1145/185595.185648

[QoS.8] Yeadon N., Mauthe A., García F., Hutchison D. (1996) “QoS filters: Addressing the heterogeneity gap”. In: Butscher B., Moeller E., Pusch H. (eds) Interactive Distributed Multimedia Systems and Services. IDMS 1996. Lecture Notes in Computer Science, vol 1045. Springer, Berlin, Heidelberg

[QoS.9] Mauthe, A., Garcia, F., Hutchison, D., Yeadon, N. “QoS Filtering and Resource Reservation in an Internet Environment”. Multimedia Tools and Applications 13, 285–306 (2001).

[QoS.10] TS 24.401

[BSW.1] Cardwell N, Savage S, Anderson T. Modelling TCP latency[C]//INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. IEEE, 2000, 3: 1742-1751.

[BSW.2] Chan K, Tong F, Chan C K, et al. An all-optical packet header recognition scheme for self-routing packet networks[C]//Optical Fiber Communication Conference. Optical Society of America, 2002: WO4.

[BSW.3] Prasad R S, Dovrolis C, Thottan M. Router buffer sizing for TCP traffic and the role of the output/input capacity ratio [J]. IEEE/ACM Transactions on Networking (TON), 2009, 17(5): 1645-1658.

[BSW.4] Khaled Salah, On the accuracy of two analytical models for evaluating the performance of Gigabit Ethernet hosts, Information Sciences, Volume 176, Issue 24, 15 December 2006, Pages 3735-3756

[BSW.5] Guido Appenzeller, Isaac Keslassy, Nick McKeown, Sizing router buffers. ACM SIGCOMM Computer Communication Review 34(4), July 2004

[BSW.6] Jingcheng Zhang, Min Zha, Lehong Niu, EBS: Electric Burst Scheduling system that supports future large bandwidth applications in scale, Proceedings of the 15th International Conference on emerging Networking EXperiments and Technologies, CoNEXT 2019, Companion Volume, Orlando, FL, USA, December 9-12, 2019.

[QUANTUM.1] P. Benioff, "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". Journal of Statistical Physics. 22 (5): 563–591. Bibcode:1980JSP....22..563B. doi:10.1007/bf01011339.

[QUANTUM.2] C. Metz, “Google Claims a Quantum Breakthrough That Could Change Computing”, New York Times, Oct 23, 2019.

[QUANTUM.3] F. Arute, et al., “Quantum supremacy using a programmable superconducting processor”, Nature | Vol 574 | 24 October 2019.

[QUANTUM.4] C. Wood, “Trump betting millions to lay the groundwork for quantum internet in the US”, CNBC.com, April 27, 2020.

———————